MANUEL DE SECURITE POUR LES INFRASTRUCTURES ROUTIERES EUROPENNES

With the financial support of the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks Programme (CIPS) European Commission – Directorate-General Home Affairs

SECMAN
Security Risk Management Processes for Road Infrastructures

Préambule

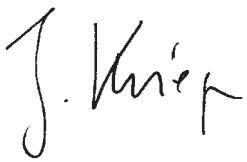
Les voies de transport internationales jouent un rôle vital pour la circulation des biens et l'approvisionnement des personnes, et elles sont nécessaires pour garantir que l'Europe reste concurrentielle. En plus d'être sûres, les routes doivent être protégées contre les attaques, catastrophes naturelles et accidents ainsi que contre toute interruption ou manipulation qui risquerait d'affecter leur niveau de disponibilité et de service.

Les infrastructures importantes comme les ponts et les tunnels s'avèrent souvent être des goulots d'étranglement. Même des interruptions minimales du trafic peuvent engendrer des « effets dominos » avec des restrictions temporaires de l'approvisionnement ayant pour conséquence des pertes économiques importantes. Les interruptions et les interventions sur ces infrastructures doivent donc, dans la mesure du possible, être courtes, exceptionnelles, relativement faciles à gérer et ne porter atteinte que dans une mesure limitée au bien-être de la population et de la société.

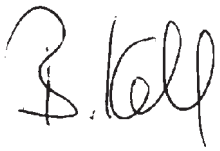
À ce jour, il n'existe aucune approche commune pour identifier, quantifier et évaluer les risques pour la sûreté des installations et identifier les éventuelles mesures de protection des infrastructures routières. Ce manuel – en tant que produit final du projet européen SecMan, se veut être une aide aux exploitants et propriétaires d'infrastructures routières européennes dans la gestion des risques et ainsi contribuer à assurer un niveau de sûreté uniforme dans toute l'Union Européenne.

De plus, le manuel soutient la stratégie de sécurité européenne en rapprochant les différents instruments, méthodologies et pratiques dans toute l'Europe. En apprenant les uns des autres et en échangeant les connaissances sur la sécurité des structures de transport en Europe, il est possible d'identifier les meilleures pratiques. Au final, c'est toute la société européenne et l'économie qui profitent d'un système de transport européen plus sûr.

Nous avons le plaisir de vous présenter les résultats de la recherche menée au cours de ces deux dernières années et espérons que vous apprécierez la lecture ainsi que l'application des principes de ce manuel. Enfin, nous aimerions remercier les membres du consortium en charge du projet pour leur coopération fructueuse et leurs contributions précieuses sans lesquelles l'élaboration de ce manuel n'aurait pas été possible.



Dr. Jürgen Krieger (BASt))



Bernhard Kohl (ILF)

Marko Žibert (ELEA)

Drago Dolenc (DARS)

Table des matières

Préambule

Acronymes

Définitions

Synthèse

PREMIÈRE PARTIE: Généralités

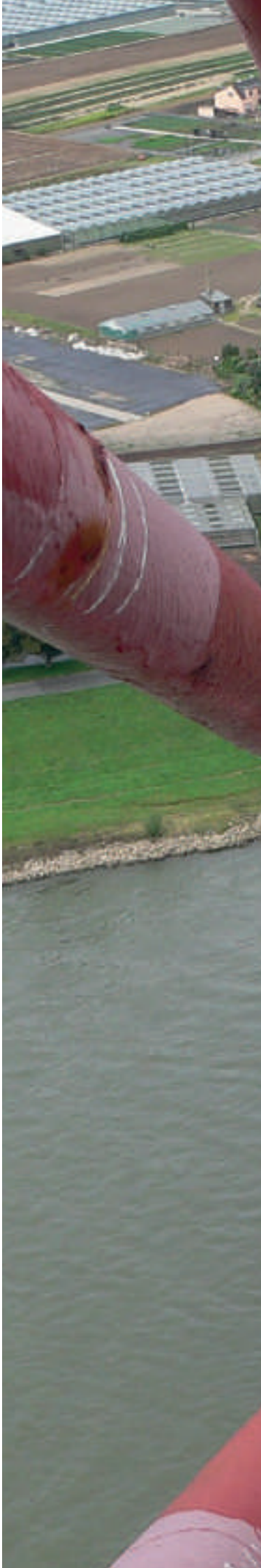
1 Introduction
1.1 Contexte et motivations
1.2 Objectif et résultats
2 Domaine d'application et limites
3 Principes
3.1 Procédure en quatre étapes
3.2 Approche à deux niveaux

DEUXIÈME PARTIE: Méthode et conseils

1 **Etape 1**
1.1 Introduction
1.2 Etape 1A: Analyse de la criticité (niveau du réseau)
1.3 Etape 1B : Evaluation de l'attractivité (niveau d'un objet)
1.4 Application pour la présélection
1.5 Autres recommandations
2 **Etape 2**
2.1 1 Introduction
2.2 Menaces
2.3 Catégorisation
2.3.1 Tunnels
2.3.2 Ponts
2.4 Analyse de la vulnérabilité
2.4.1 Faisabilité d'une attaque
2.4.2 Dommages potentiels
2.4.3 Résultat
2.5 Autres recommandations
3 **Etape 3**
3.1 Introduction
3.2 Méthodologie
4 **Etape 4**
4.1 Introduction
4.2 Catégorisation des mesures
4.3 Processus de sélection des mesures
4.4 Autres recommandations

TROISIÈME PARTIE 3 : Exemple pratique

QUATRIÈME PARTIE: Liste des mesures



Acronymes

TMJA	Trafic moyen journalier annuel
BLEVE	Explosion due à la présence de vapeur libérée par des liquides en ébullition
CAV	Criticité – Attractivité - Vulnérabilité
IC	Infrastructure critique
PIC	Protection des infrastructures critiques
MD	Matières dangereuses
DP	Dommages potentiels
IEC	Infrastructures européennes critiques
PEPIC	Programme européen pour la protection des infrastructures critiques
EM UE	Etat membres de l'UE
RA	Risque d'attaque
PL	Véhicule poids lourd
EEI	Engin explosif improvisé
ISO	Organisation internationale de normalisation
TI	Technologie de l'information
AIT	Association internationale des tunnels
NMA	Nouvelle méthode autrichienne pour le percement de tunnel
RABT	« Richtlinien für die Ausstattung und den Betrieb von Straßentunneln » (Directives pour l'équipement et l'opération des tunnels routiers ; documentation allemande)
SeRoN	Projet « Security of Road Transport Networks » : projet de recherche sur la sécurité des réseaux de transport routiers
SKRIBT	« Schutz Kritischer Brücken und Tunnel im Zuge von Straßen » (Protection des ponts et tunnels critiques du réseau routier)
TBM	Tunnelier
TEN-T	Réseau de transport transeuropéen
Lot	Ensemble de tâches

Définitions

Terme	Définition	Source
Actif	Elément de valeur ou important. Les actifs peuvent comprendre les éléments physiques, cyber-éléments (systèmes d'information et de communication), les éléments vivants ou humains (savoir-faire et fonctions critiques).	**SeRoN**
Conséquence	Résultat d'un événement en termes de dommages sur la santé des personnes, la propriété ou l'environnement.	**SeRoN**
Analyse des conséquences	Procédure systématique décrivant et/ou calculant les conséquences.	**PIARC**
Méthode de construction	La méthode de construction d'un tunnel, soit conventionnelle/ par tunnelier, tranchée couverte ou immersion	**SecMan**
Personnel chargé du contrôle	Tous les employés chargés de la gestion du trafic et/ou des aspects techniques	**PIARC**
Infrastructure critique	Actif entier ou partiel essentiel au maintien des fonctions sociétales vitales, de la santé, la sécurité, de l'économie ou du bien-être social des personnes et dont l'arrêt ou la destruction pourrait avoir un impact important en cas d'impossibilité à maintenir de ces fonctions (cf. [EC, 2008])	**SeRoN**
Situation critique	Situation (encombrement, panne, accident, incendie) exigeant une attention spécifique ou une action des utilisateurs	**PIARC**
Criticité	La criticité renvoie au réseau de transport, en indiquant l'importance d'une section de réseau particulière pour le fonctionnement de l'ensemble du réseau de transport. Par conséquent, une structure peut être vulnérable à une menace spécifique mais pas critique pour le réseau si elle se situe sur une section non critique. D'autre part, cette section peut être critique pour le fonctionnement du réseau mais moins vulnérable à une menace donnée.	**SecMan**
Détection	L'action d'être conscient de l'occurrence d'un événement (généralement, la détection peut être humaine (vue, ouïe, odorat…) ou dépendre d'un système (chaleur, détection automatique d'incident, niveau CO…)	**PIARC**
Urgence	Evénement soudain et imprévu exigeant une action immédiate pour prévenir les menaces potentielles sur la santé, la sécurité, l'environnement et les biens.	**PIARC**
Plan d'opération d'urgence	Plan détenu par chaque service, agence ou entité exploitant le tunnel et mis à jour régulièrement pour répondre de manière appropriée aux situations d'urgence.	**PIARC**
Préparation à l'urgence	Il s'agit de la discipline qui assure qu'une entité est prête à répondre en situation d'urgence de manière coordonnée, efficace et en temps opportun.	**PIARC**
Services de secours	Pompiers, Police, et services médicaux d'intervention	**PIARC**
Evénement	Occurrence d'un ensemble de circonstances particulières risquant de causer des dommages.	**PIARC**
Mesures de sécurité graduées	Mesures qui peuvent être déclenchées en fonction de différents niveaux de menace	**2008/114/CE**
Fréquence	Nombre de fois qu'un événement donné a lieu durant un intervalle particulier (ex. nombre d'accidents par an).	**PIARC**
Dommages	Blessures physiques ou dommages infligés à la santé des personnes, aux biens ou à l'environnement.	**PIARC**
Danger	Source potentielle de dommages	**PIARC**
Conditions hydro-géologiques	Conditions de l'eau sous la surface de la terre et les aspects géologiques liés.	**SecMan**

Incident	Evénement anormal et non prévu (y compris les accidents) ayant des effets négatifs sur le fonctionnement des tunnels et la sécurité	**PIARC**
Mesures de sécurité permanentes	Mesures identifiant les investissements et moyens nécessaires en matière de sûreté qui sont susceptibles d'être utilisés en toutes circonstances. Elles contiennent des informations relatives aux mesures générales, par exemple les mesures techniques (y compris l'installation de moyen de détection, de contrôle d'accès, de protection et de prévention), les mesures organisationnelles (y compris les procédures d'alerte et de gestion de crise), les mesures de contrôle et de vérification, aux communications, à la sensibilisation et à la formation, ainsi qu'à la sécurité des systèmes d'information.	**2008/114/EC**
Conditions géotechniques prédominantes	Conditions géotechniques du milieu autour du tunnel, généralement des roches stables ou des terrains meubles.	**SecMan**
Probabilité	Risque qu'un événement survienne, exprimé par un nombre compris entre 0 et 1.	**PIARC**
Analyse de la probabilité	Procédure systématique pour décrire et/ou calculer la probabilité d'un événement futur.	**PIARC**
Analyse quantitative des risques	Méthode d'analyse des risques basée sur les calculs numériques.	**PIARC**
Risque	Combinaison de la probabilité d'apparition de dommages et de la sévérité des dommages (ISO IEC 51).	**PIARC**
Analyse des risques	Utilisation systématique des informations disponibles pour identifier les dangers et estimer les risques.	**PIARC**
Gestion des risques	Processus systématique mis en place par une organisation pour atteindre et maintenir un niveau de risque tolérable.	**PIARC**
Réseau routier	Système complet de routes destiné au transport routier, à disposition dans un espace donné ; plus généralement, l'ensemble du réseau dont les utilisateurs de ce manuel ont la responsabilité.	**SecMan**
Section du réseau routier	Partie définie d'un réseau routier comprenant un ensemble de routes.	**SecMan**
Section de route	Partie définie d'un réseau routier sur la base des différences dans les paramètres de trafic.	**SecMan**
Sécurité	Protection des structures de transport vis-à-vis des événements non-intentionnels comme les accidents, couverte par les normes applicables.	**SecMan**
Sûreté	Disposition, protection et préservation des structures de transport contre les événements intentionnels.	**SecMan**
Scénario	Combinaison d'événements, états des systèmes et conditions donnant lieu à un résultat pertinent. Ces événements et conditions peuvent être utilisés dans une analyse des risques ou autres modèles. Cela peut comprendre par exemple une menace spécifique pour un actif ou objet, avec les probabilités et conséquences associées.	**SeRoN**
Enveloppe simple/double	Dans un tunnel à enveloppe simple, il n'y a qu'une seule paroi. Dans un tunnel double, l'enveloppe est constituée d'une première paroi externe (béton projeté) et d'une paroi interne (béton in-situ)	**SecMan**
Cellule simple/multiple	Dans un tunnel à section rectangulaire, les cellules pourront être divisées par un mur de séparation en plusieurs cellules.	**SecMan**
Section de tablier (Pont)	Tous les éléments d'un pont qui supportent les charges, et qui sont situés au-dessus des appuis du pont sont considérés comme le tablier. Ils soutiennent le trafic.	**SecMan**
Système (pont)	**Système statique d'un pont définissant la méthode de conception d'un pont.**	**SecMan**

Menace	Tout type de circonstance ou événement risquant de causer la perte ou des dommages sur un actif. En cas de menace terroriste, la menace représente l'intention et la capacité combinées à l'attractivité d'un actif par rapport aux autres actifs. En cas de dangers naturels, la menace renvoie à la fréquence historique ou estimée de l'événement naturel auquel l'actif peut être exposé. Dans les deux cas, l'analyse des risques a pour objectif de définir la probabilité d'un événement.	**SeRoN**
Centre de contrôle du tunnel	Centre opérationnel dédié au contrôle et à la coordination des opérations d'un tunnel et au maintien, là où nécessaire, de la communication entre le personnel exploitant et les autres agences concernées	**PIARC**
Vulnérabilité	Caractéristiques et circonstances d'une communauté, d'un système ou d'un actif le rendant sensibles aux effets dévastateurs d'un danger (menace, événement). La vulnérabilité est liée la notion de risque en cas d'événement ou de scénario particuliers.	**SeRoN**

Synthèse

Le transport fait partie des secteurs les plus importants pour l'économie et la société européenne dans son ensemble. Ses infrastructures sont essentielles pour le bon fonctionnement de la totalité du réseau. Les propriétaires et exploitants de ces infrastructures doivent aujourd'hui faire face à de nombreux défis pour assurer la bonne opération du trafic sous leur responsabilité. Ces défis peuvent aller du trafic normal aux accidents en passant par des interruptions majeures dues à des attaques intentionnelles.

Le présent manuel aborde plus précisément le thème de la protection des infrastructures routières, comme les tunnels et les ponts, contre les attaques humaines intentionnelles. Il décrit une procédure en 4 étapes permettant l'évaluation des infrastructures par rapport à leur criticité pour le réseau, leur attractivité pour une attaque et leur vulnérabilité. Cette approche permet à l'utilisateur d'identifier les points faibles du réseau routier au regard des nombreux dangers et de faciliter la décision de porter plus d'attention à un nombre réduit d'éléments à haut risque, attractifs pour une attaque et vulnérables. De plus, différentes mesures de protection sont présentées et définies sous forme de matrice de comparaison, permettant à l'utilisateur de choisir la meilleure solution au cas par cas.

L'approche ouverte et holistique de la méthodologie permet son application à l'échelle européenne, contribuant ainsi à la sûreté des infrastructures de transport et donc à celle des artères européennes.

Première Partie: Généralités

Première Partie: Généralités

La section suivante présente le contexte, les motivations, l'objectif et les apports de ce manuel ainsi que son champ d'application et ses limites. De plus, il présent les trois principes fondateurs de la méthodologie.

1. Introduction

Ce manuel a été élaboré pour les propriétaires et exploitants d'infrastructures routières afin qu'ils puissent évaluer leurs infrastructures par rapport aux risques de sûreté et identifier des mesures potentielles de protection. Ce manuel est prêt à l'emploi, il permet à l'utilisateur de développer une bonne compréhension des risques sécuritaires pesant sur son réseau. Il en résulte une évaluation globale des structures routières analysées donnant à l'utilisateur une première indication des structures potentiellement critiques ou vulnérables et lui indiquant quelles mesures pourraient être mises en place pour gérer les problèmes.

1.1 Contexte et motivations

TLes voies de transport internationales jouent un rôle primordial pour la circulation des biens et l'approvisionnement des personnes. Dans ce contexte, les infrastructures sensibles comme les ponts et les tunnels peuvent représenter des goulots d'étranglement dont tout dysfonctionnement pourrait avoir des impacts négatifs sur la population ainsi que sur l'économie. Jusqu'à présent, aucun manuel directement applicable n'a abordé la sûreté de ces infrastructures. Toutefois, il apparait aujourd'hui nécessaire d'harmoniser l'identification des infrastructures routières critiques et vulnérables en Europe. Les différences au niveau des normes et des équipements de sécurité ainsi que la méconnaissance des sections ou structures importantes sur les réseaux routiers à travers l'Europe peuvent avoir des impacts négatifs sur la sécurité des routes et donc sur la chaîne logistique au sein de l'économie européenne.

Depuis les événements du 11 Septembre 2001, le terrorisme et autres menaces sécuritaires, ont gagné en importance dans différents secteurs en Europe, les infrastructures routières étant des cibles faciles avec des conséquences potentiellement énormes pour les propriétaires, utilisateurs et la société dans son ensemble. Depuis, de nombreux projets de recherche ont été menés sur l'identification et l'évaluation des infrastructures de transport vulnérables par rapport aux différentes menaces [SeRoN, SKRIBT]. Toutefois, les résultats de ces projets de recherche ne sont pas encore appliqués dans les activités de tous les jours des propriétaires et exploitants de ces infrastructures. Ce manuel a pour objectif de combler le vide entre la théorie et la pratique et présente un guide prêt à l'emploi sur comment identifier et évaluer les sections d'autoroutes et structures existantes à risque et donne une première indication sur quelles mesures pourraient être mises en place pour réduire les dommages potentiels d'une menace particulière sur une structure routière ou une section d'autoroute. De manière plus générale, ce manuel a pour dessein de contribuer au renforcement de la résilience du réseau de transport européen vis-à-vis des différents dangers d'origine humaine et d'accroitre la sensibilité des propriétaires et exploitants des installations routières pour ces types de dangers.

1.2 Objectif et résultats

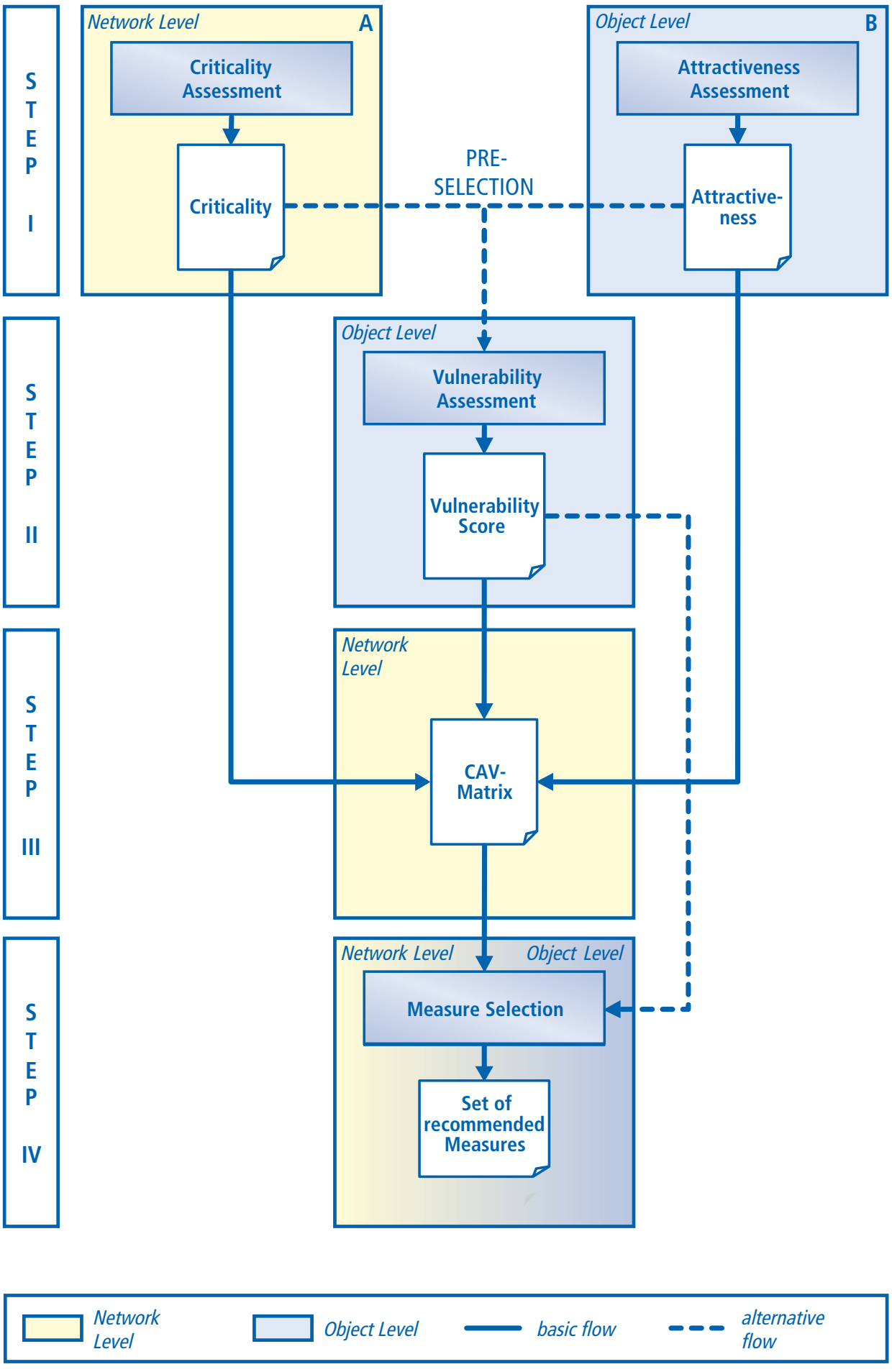
Dans la logique des directives européennes récemment publiées [2008/114/CE], ce manuel contribue aux efforts Européens pour la mise au point d'une méthodologie commune et harmonisée pour l'identification des infrastructures critiques et des mesures de sécurité adéquates. Il fournit aux propriétaires et exploitants de route un outil simple et pratique pour l'évaluation de leurs infrastructures. De plus, il propose une approche basée sur les risques pour évaluer les infrastructures routières tout en identifiant en même temps les possibilités d'analyses complémentaires détaillées quantitatives et approfondies.

Un autre apport de ce manuel est qu'il favorise le débat entre la théorie et la pratique. Comme indiqué ci-dessus, un grand nombre de projets de recherche ont été menés sur ce thème. Mais nombreuses sont les difficultés pour en appliquer les résultats au quotidien. C'est pourquoi, l'approche de ce manuel se veut aussi détaillée que possible tout en restant relativement facile à mettre en œuvre dans la pratique et a été conçu pour être applicable dans toute l'Europe. Même si cela a conduit nécessairement à une limitation du niveau de détail de l'évaluation, cela rend les résultats comparables et favorise l'harmonisation des pratiques à travers l'Union Européenne.

2. Domaine d'application et limites

De manière générale, la méthodologie présentée propose une évaluation holistique des structures routières par rapport à leur criticité, leur vulnérabilité et aux mesures de sécurité potentielles. Même si elle est applicable dans toute l'Europe, la méthodologie présentée comporte certaines limites concernant son champ d'application, les menaces abordées et les structures prises en considération. De manière générale, ce manuel se concentre sur les infrastructures routières telles que les ponts et les tunnels. Ces infrastructures ont été catégorisées afin que la méthode soit la plus détaillée possible tout en restant aussi concise que nécessaire dans son application. Dans le

» Schéma 1 – Diagramme de la méthodologie



cadre d'une évaluation holistique de la sécurité, d'autres structures techniques peuvent aussi dans certains cas être importantes. Toutefois, en considérant avant tout les principales infrastructures routières (ponts et tunnels), ce manuel de sécurité donne une première indication sur les structures les plus pertinentes d'un réseau routier.

En outre, seuls les risques d'origine humaine sont pris en compte. Cela signifie que les menaces et risques naturels comme les conditions climatiques extrêmes ou les accidents mineurs ne sont pas intégrés à l'étude. De plus, rappelons que les scénarii étudiés ne comprennent pas les cyber-attaques/menaces. Même si le risque concernant ce type d'évènements devrait être de plus en plus important dans les années à venir, d'autres études plus détaillées sont nécessaires pour évaluer de manière adéquate l'impact des cyber-attaques sur les infrastructures routières. L'approche de ce manuel se concentre avant tout sur la disponibilité du réseau routier. C'est pourquoi seules les menaces risquant d'endommager les structures en elles-mêmes ont été considérées. Cela signifie que toutes les menaces n'ayant d'impacts que sur les utilisateurs des structures ne font pas partie de la présente méthodologie. Par ailleurs, aucune combinaison de menaces, comme par exemple une explosion accompagnée d'une contamination par une substance dangereuse n'est pas intégrée au projet. Tout au long du développement des scénarii pertinents résultant des menaces identifiées, seuls les plus importants en termes de conséquences ont été pris en compte.

Pendant le processus de sélection des mesures, aucune quantification de l'efficacité des mesures n'est donnée. Aussi, ces groupes de mesures doivent être vus comme une première indication sur ce qui pourrait être fait. D'autres recommandations sont énoncées lorsque cela apparait judicieux. Les effets combinés des mesures ne sont pas inclus dans le processus de sélection.

En résumé, le présent manuel donne aux utilisateurs une première indication sur la criticité et la vulnérabilité de ses infrastructures routières. Une analyse détaillée pourra être nécessaire, en fonction des situations au cas par cas.

3. Principes

Ce manuel suit deux principes de base :

La méthodologie suit une procédure en quatre étapes, dans laquelle chaque étape peut être exécutée individuellement ou en combinaison avec les autres.

De plus, le manuel utilise une approche à deux niveaux, ce qui signifie que l'évaluation globale des infrastructures peut être assurée en appliquant cette méthodologie sur une base semi-quantitative (niveau 1), tout en gardant à l'esprit que les investigations détaillées et spécifiques aux objets ne font pas partie de ce manuel mais pourront être nécessaires afin d'évaluer l'intégralité du réseau de transport (niveau 2).

En général, ce manuel est basé sur des avis d'experts. Les valeurs par défaut indiquées ont été définies par le projet SecMan au cours de séminaires internes et externes auxquels ont participés des experts en infrastructures routières provenant de différentes spécialités. Ces valeurs pourront être ajustées par les utilisateurs si les spécificités du cas considéré l'exigent.

3.1 Procédure en quatre étapes

La méthodologie du manuel de sécurité pour les infrastructures routières européennes est divisée en quatre étapes. L'étape 1 comprend l'évaluation de l'attractivité et de la criticité, l'étape 2 couvre l'analyse de la vulnérabilité et l'étape 3 combine les résultats des deux étapes précédentes dans une matrice globale. Enfin, l'étape 4 présente les mesures de protection et d'atténuation pour les objets identifiés.

Les procédures d'évaluation sont menées soit au niveau du réseau soit au niveau de l'objet. Au cours des évaluations au niveau du réseau, seule une partie du réseau comportant éventuellement plusieurs sections est considérée. Au niveau d'un objet, des objets singuliers sont vérifiés avec des paramètres plus spécifiques.

3.2 Approche à deux niveaux

La méthodologie est divisée en deux niveaux de détails. La méthodologie présentée dans le schéma (schéma 1) agit au niveau 1, ce qui signifie qu'elle donne une première vue d'ensemble de la criticité de certaines sections ou de la vulnérabilité de certains objets sur un réseau routier donné. Toutefois, tout au long de cette méthode, plusieurs points apparaissent qui nécessitent une étude plus détaillée pour obtenir une analyse approfondie et holistique du réseau routier et/ou de ses infrastructures. Pour cela, des recommandations sont données sur les procédures ou analyses les plus efficaces ou les plus utiles dans les différents cas.

Deuxième Partie: Méthode et conseils

1. Etape 1

1.1 Introduction

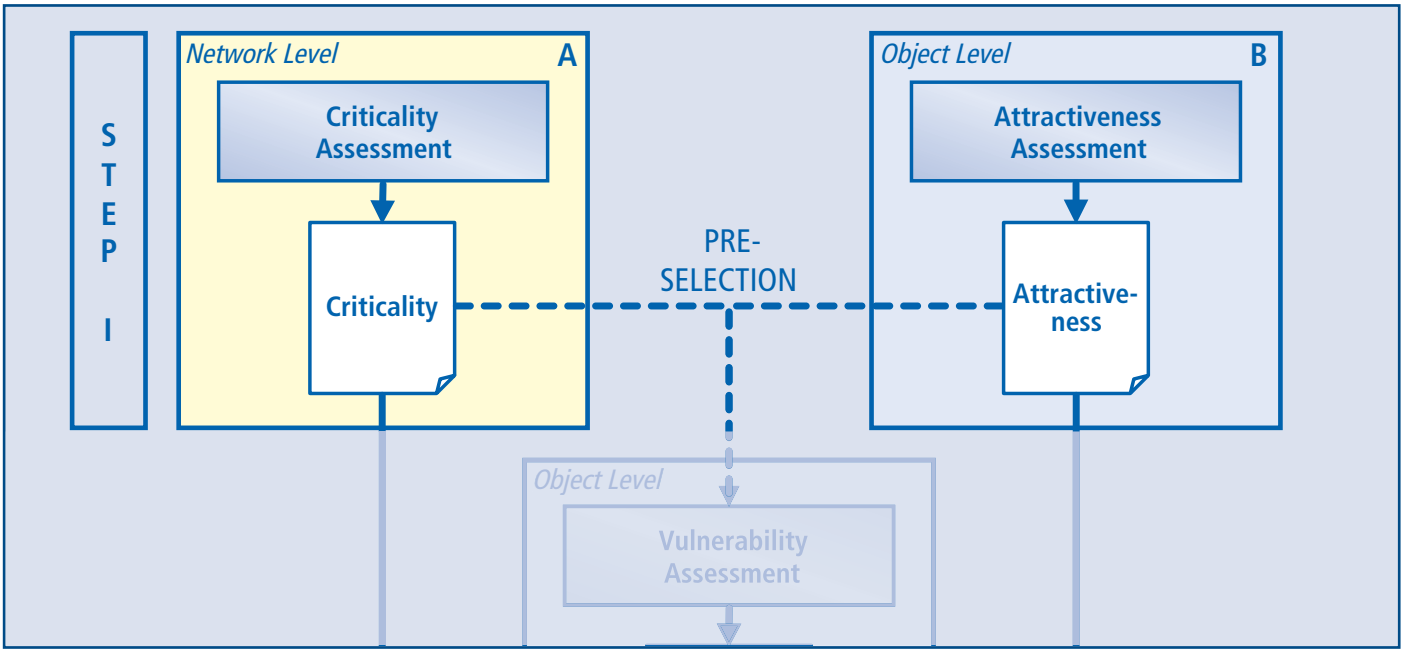
La méthodologie développée par le projet SecMan est un outil d'aide à la décision qui permet aux propriétaires et exploitants des réseaux routiers de vérifier les ponts et les tunnels de leur réseau routier vis-à-vis des risques potentiels en matière de sûreté. Cette méthodologie est facile à appliquer et repose sur des données d'infrastructures généralement disponibles pour l' utilisateur. Toutefois, elle doit être appliquée dans le contexte de la stratégie spécifique de l'exploitant / du propriétaire en matière de sûreté pour le réseau routier concerné. Pour les prises de décisions finales, l'utilisateur doit, en plus des résultats de la méthodologie, définir ses propres priorités en fonction des objectifs stratégiques suivis/souhaités.

Pour appliquer la méthodologie, il convient de choisir la partie du réseau routier à étudier. La taille du réseau dépend du champ d'investigation de l'étude.

La première étape de la méthode est divisée en deux sous-étapes : étape 1A (analyse de la criticité) et étape 1B (analyse de l'attractivité), qui peuvent être menées en parallèle. Ces deux étapes utilisent une procédure d'évaluation qualitative simple et leurs résultats – « criticité » et « attractivité » - sont des paramètres très importants pour les étapes suivantes de l'analyse.

De plus, les deux procédures d'évaluation peuvent être utilisées comme méthode de présélection pour réduire le nombre d'objets à étudier dans le cadre de l'évaluation plus détaillée de la vulnérabilité, à l'étape 2.

» Schéma 2 – Etape 1 (Analyse de la criticité et de l'attractivité)



1.2 Etape 1A: Analyse de la criticité (niveau du réseau

Un réseau routier comprend plusieurs sections qui sont importantes pour la disponibilité et le niveau de service de l'ensemble du réseau. Dans cette étape, chaque section de la partie choisie du réseau est évaluée sur la base d'une série de paramètres de trafic. Pendant l'évaluation, chaque section du réseau routier doit être évaluée en fonction de sa « criticité » en utilisant une procédure d'analyse qualitative simple reposant sur un système de « feux » (cf. schéma 3). La criticité est un indicateur de l'importance du fonctionnement de la dite section au sein du réseau routier.

Les paramètres de trafic utilisés pour l'évaluation peuvent aussi servir pour diviser le réseau en sections.

- very critical
- critical
- less critical

» Schéma 3: Paramètres pour l'évaluation de la criticité

L'évaluation peut être réalisée à partir des paramètres du réseau suivants :

1. Itinéraires de contournement

La section du réseau est plus importante si elle ne dispose d'aucun

itinéraire de contournement ou bien s'ils sont peu appropriés. Ces déviations ne sont appropriées que si le temps de trajet sur la nouvelle route n'est pas considérablement plus long et si elle peut supporter le trafic dévié en plus de l'existant en termes de volume et type de trafic

2. Trafic moyen journalier annuel (TMJA)

Sur une section de réseau routier donnée, plus le trafic mesuré en volume est important (c'est-à-dire plus le TMJA est élevé), plus la section est importante.

3. Véhicules utilitaires poids lourds

Plus le pourcentage de poids lourds dans le trafic d'une section est élevé, plus cette section est importante pour le réseau de transport. Un nombre élevé de véhicules poids lourds peut par exemple indiquer que cette section routière est économiquement très importante.

4. Transport spécial

Le transport par poids lourds est qualifié de spécial lorsqu'il requiert certaines autorisations particulières pour des types d'objets et qu'il n'est parfois pas autorisé à franchir certaines infrastructures. Dans certains tunnels par exemple, le transport de matières dangereuses est règlementé ou bien encore interdit; de même sur certains ponts.

Ces quatre paramètres sont proposés ici par défaut. Il est possible d'ajouter d'autres paramètres individualisés ou de réaliser l'évaluation en fonction d'une sélection de paramètres proposés. Si certaines sections de réseau (très) critiques sont déjà identifiées/connues, cette étape peut être ignorée.

De plus, aucune valeur limite, par exemple pour le TMAJ ou pour le pourcentage de poids lourds dans le trafic, n'est proposée. Généralement, ces valeurs dépendent fortement du trafic sur le réseau considéré et diffèrent d'un pays à l'autre.

Cette approche simple permet de diviser le réseau routier en plusieurs sections affichant des criticités différentes à partir des paramètres mentionnés plus haut. De cette manière, on obtient au premier abord un aperçu de la localisation (dans quelle région) des sections les plus critiques et cela permet de classer les sections dans le réseau. Cette analyse facilite ainsi les prises de décisions en attribuant la priorité aux sections où des évaluations supplémentaires sont nécessaires.

1.3 Etape 1B : Evaluation de l'attractivité (niveau d'un objet)

Au niveau de l'étape 1B, une évaluation du niveau d'attractivité d'un objet spécifique est réalisée. L'histoire récente montre qu'il existe certains facteurs qui pourraient augmenter la faisabilité d'une attaque terroriste et pousser des malfaiteurs à l'action en raison par exemple de l'attention médiatique qui en résulterait.

Chaque objet (potentiellement attractif) doit être évalué en fonction de son attractivité en utilisant une procédure simple d'analyse quantitative reposant sur un système de « feux » (cf. schéma 4). Plus un objet est attractif pour un malfaiteur, plus la probabilité d'être attaqué est élevée, et donc une évaluation supplémentaire est recommandée.

Toutefois, l'évaluation de l'attractivité est seulement une procédure

» Schéma 4: Paramètres pour l'évaluation de l'attractivité

subjective. Pour améliorer la qualité des résultats, il est conseillé de faire appel à plusieurs experts de différentes disciplines pour l'évaluation de l'attractivité. Pour aider les spécialistes, les 3 paramètres suivants peuvent être utilisés comme points de départ :

1. Valeur symbolique

L'objet peut ne pas se trouver sur une route très importante, mais être très connu dans le pays voire à l'étranger. Une attaque donnerait probablement lieu à une forte couverture médiatique dans le monde entier.

2. Nombre de décès important en raison de l'effondrement de l'infrastructure

Le niveau d'attractivité augmente si l'attaque d'un objet ou de l'un de ses systèmes occasionne de nombreux décès, à l'intérieur, sous ou sur l'infrastructure.

3. Effets secondaires

Un objet peut être plus attractif pour une attaque si des effets secondaires de l'attaque influencent par exemple d'autres modes de transport proches de l'infrastructure.

Ces trois paramètres sont proposés ici par défaut. Il est possible d'ajouter d'autres paramètres individualisés ou de réaliser l'évaluation en fonction d'une sélection de paramètres proposés. Si certains objets (très) attractifs sont déjà identifiés ou connus, cette étape peut être ignorée.

1.4 Application pour la présélection

Les deux processus d'évaluation de l'étape 1 peuvent servir de présélections pour l'évaluation de la vulnérabilité. Dans la pratique, les parties de réseau routier étudiées peuvent inclure un grand nombre d'objets, ce qui conduirait ainsi à une étape 2 très longue voire fastidieuse. En utilisant des présélections, les objets peuvent être filtrés et le nombre d'objets à analyser réduit. Les objets moins attractifs et/ou les sections de routes moins critiques n'ont pas besoin d'être pris en considération dans les étapes ultérieures de l'analyse. De plus, il est recommandé d'exclure les ponts de moins de 10-12 m de portée. Dans la pratique, ils peuvent être remplacés très rapidement par des ponts mobiles.

1.5 Autres recommandations

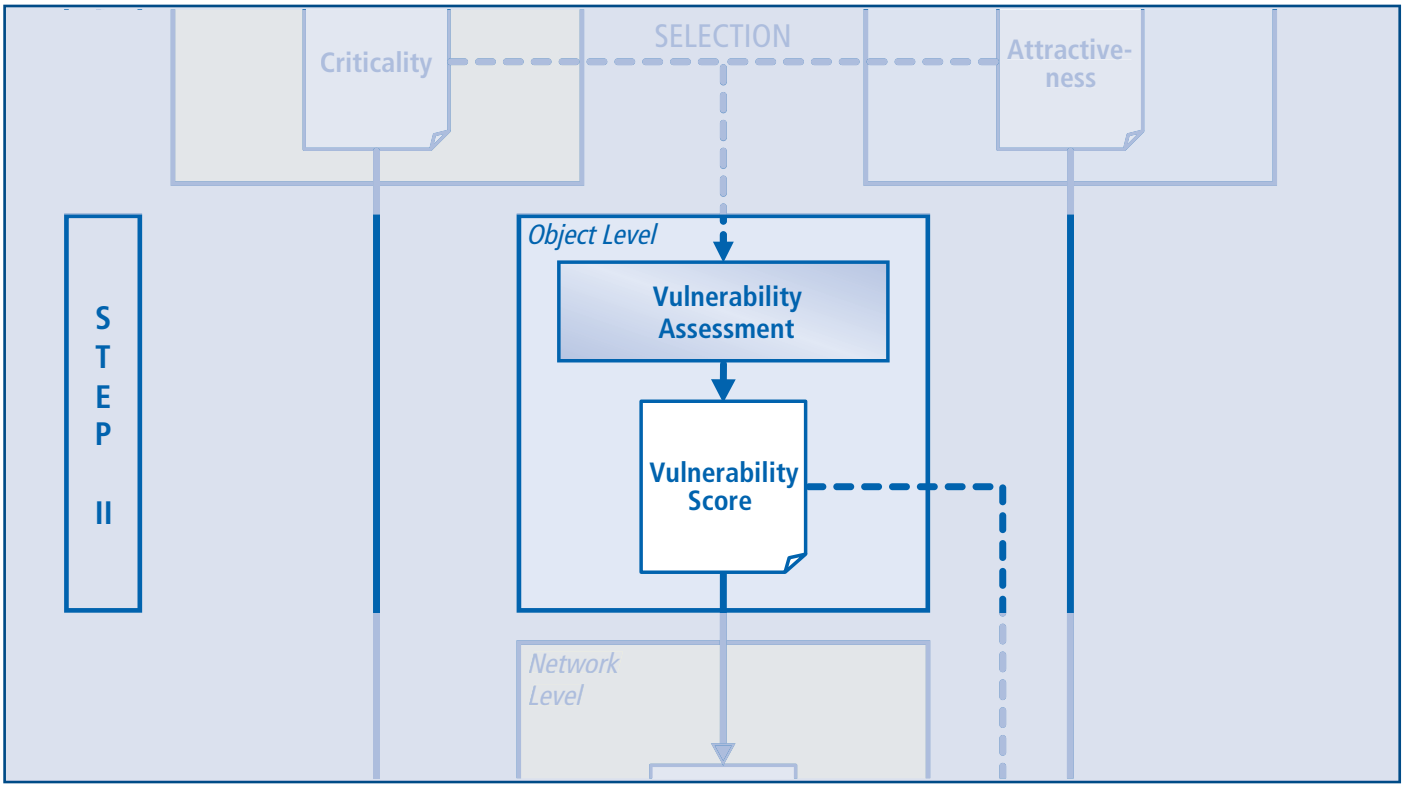
Si les procédures d'analyse qualitative de l'étape 1 ne sont pas suffisantes, les méthodes suivantes peuvent être utilisées pour une analyse plus approfondie (niveau 2). Par exemple, une analyse détaillée du réseau routier avec un modèle numérique fin du transport et du trafic peut être développée pour analyser le réseau et évaluer la criticité de chaque section de route.

2. Etape 2

2.1 Introduction

L'étape 2 est une évaluation appelée analyse de la vulnérabilité (voir schéma 5). Elle est réalisée à l'échelle de l'objet pour un tunnel ou un pont et concerne certains types de menaces. D'une part, cette étape peut être utilisée individuellement pour évaluer un objet particulier. D'autre part, elle peut aussi être utilisée comme l'une des quatre étapes de l'évaluation globale d'un réseau. Toutefois, il est recommandé d'utiliser l'étape 1 comme présélection afin de réduire le nombre d'objets à analyser plus en détail dans l'étape 2.

Le résultat de cette étape est une valeur quantitative appelée « valeur de vulnérabilité », un critère essentiel pour les procédures d'évaluation suivantes.



» Schéma 5 – Etape 2 (Analyse de la vulnérabilité)

En matière de sécurité routière, le terme de « risque » est souvent utilisé. Il est calculé en multipliant les chances (ou probabilité) qu'un événement particulier se produise, et son impact (ou conséquence) directe (c'est l'équation du risque). Dans le cadre de ce manuel, une équation similaire est utilisée pour définir la vulnérabilité comme étant le produit de la faisabilité d'une attaque et des dommages potentiels.

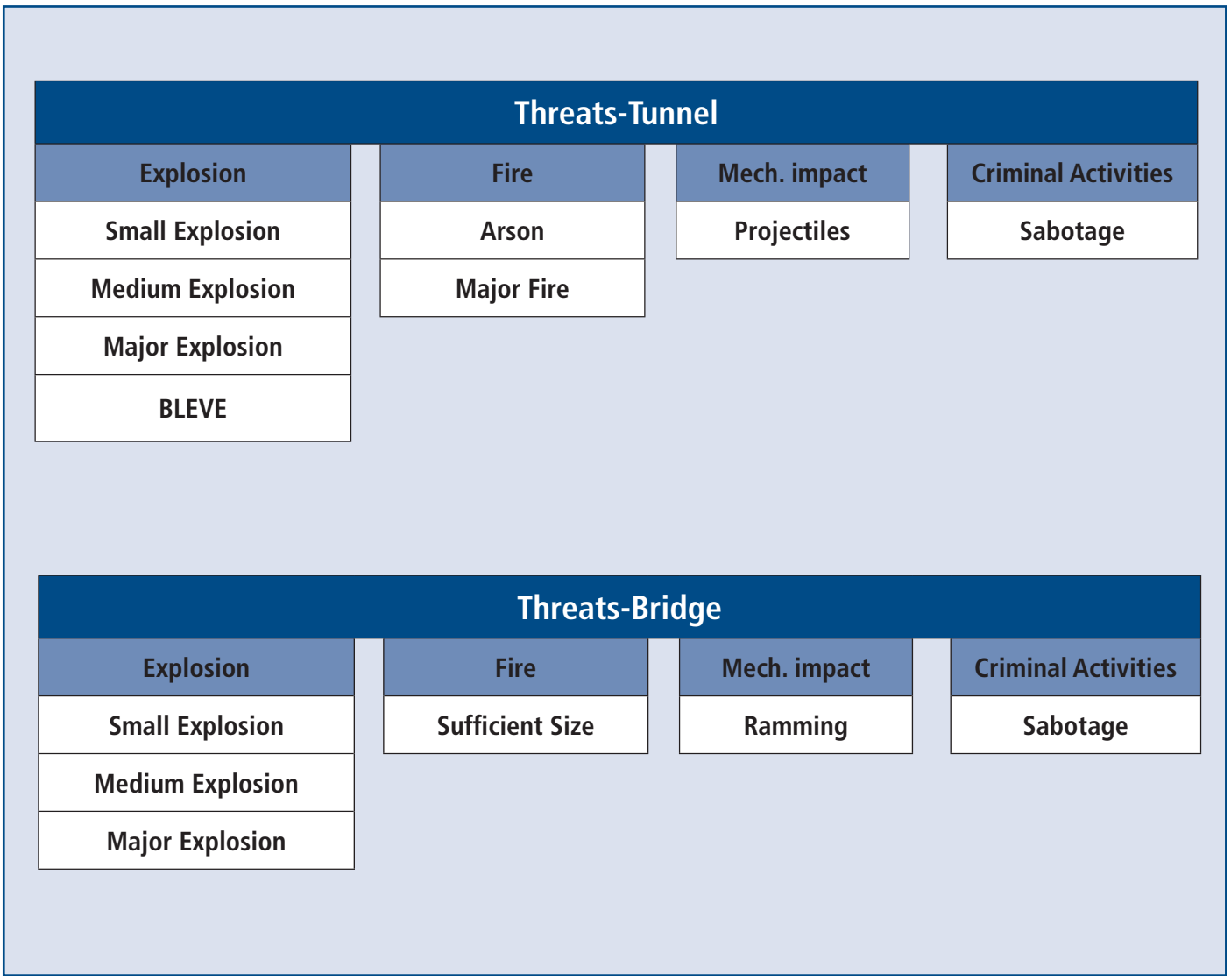
Pour ce qui est de la sûreté, il n'est pas vraiment possible de définir la probabilité d'un événement intentionnel. C'est pourquoi le terme de « faisabilité d'une attaque » a été introduit. Elle est déterminée à partir de plusieurs aspects comme la complexité d'une attaque et la capacité de l'attaquant. Concernant les conséquences d'une menace intentionnelle, les effets résultant d'un scénario très défavorable pour la structure sont à prendre en compte. Ainsi, les dommages potentiels couvrent les dommages matériels potentiels et sont quantifiés par la durée jusqu'à la remise en service de l'objet considéré (« durée de la période hors-service »).

Le schéma 6 présente la transition entre la probabilité, les conséquences et le risque vers la faisabilité d'une attaque, les dommages potentiels et la vulnérabilité – de la sécurité vers la sûreté.

» Schéma 6: Risque vs. Vulnérabilité

2.2 Menaces

Comment indiqué auparavant, l'analyse de la vulnérabilité est une procédure d'évaluation des tunnels et/ou ponts par rapport à certains types de menaces. Au total, quatre types de menaces sont considérés comme pertinents et adaptés pour les deux familles d'objets, certains types étant divisés en sous-types (cf. schéma 7).



» Schéma 7: Ensemble des menaces potentielles pour les tunnels et les ponts

Dans le cas des tunnels, les explosions et gros incendies à l'intérieur des galeries sont pertinents. Les incendies criminels, projectiles et sabotages sont seulement pertinents pour les centres opérationnels locaux des tunnels ainsi que pour les installations de ventilation des systèmes d'extraction des fumées. Si un tunnel dispose de l'une de ces infrastructures particulières, la vulnérabilité de ces objets associés doit être ajoutée à la vulnérabilité du tunnel respectif.

De plus, pour chaque type de menace, un scénario très défavorable a été retenu pour définir les valeurs par défaut des fiches utilisateurs. En raison du caractère très sensible des informations sur les points faibles d'un tunnel ou d'un pont, ces scénarii référence ne sont pas publiés dans le présent manuel.

2.3 Catégorisation

Dans la pratique, une grande variété de tunnels et de ponts existe, chaque objet ayant des caractéristiques spécifiques. Pour évaluer ces infrastructures et faciliter la compréhension, les infrastructures sont réparties en quelques catégories type représentatives. Les critères de catégorisation des tunnels et des ponts sont très différents. C'est pourquoi ils sont présentés séparément.

2.3.1 Tunnels

Le tableau 8 montre la catégorisation des tunnels à partir des 5 critères suivants :

- Conditions géotechniques prédominantes
- Méthode de construction (conventionnelle/NMA, tunnelier)
- Conditions hydrogéologiques
- Enveloppe simple ou double
- Cellules simples/multiples.

De plus, l'existence de centres opérationnels locaux et de systèmes de ventilation pour l'extraction des fumées a été considérée comme pertinente pour un tunnel. Pour certains types d'attaque (ex. sabotage), ces composants sont essentiels pour une exploitation sûre du tunnel dans son ensemble. En incluant ces deux composants associés au tunnel, la catégorisation aboutit à un total de vingt types de tunnels.

Predominant Geotechnical Conditions	Construction Method	Hydrogeological Conditions	Single/Dual Shell	Single/Multiple Cell	Type No.
Rock, Stable without Support	Conventional or TBM	Dry, only Minor Water Ingress	Single Shell	-	T01
			Dual Shell	-	T02
		Considerable Water Ingress, Risk of Flooding	Single Shell	-	T03
			Dual Shell	-	T04
Weak Rock, Loose Ground, Soft Soil, Instable without Support	Conventional or TBM	Dry, only Minor Water Ingress	Single Shell	-	T05
			Dual Shell	-	T06
		Considerable Water Ingress, Risk of Flooding	Single Shell	-	T07
			Dual Shell	-	T08
	Cut and Cover	Dry, only minor Water Ingress	Single Shell	Single Cell	T09
				Multiple Cell	T10
			Dual Shell	Single Cell	T11
				Multiple Cell	T12
		Considerable Water Ingress, Risk of Flooding	Single Shell	Single Cell	T13
				Multiple Cell	T14
			Dual Shell	Single Cell	T15
				Multiple Cell	T16
	Immersed Tunnel	Considerable Water Ingress, Risk of Flooding	Single Shell	Single Cell	T17
				Multiple Cell	T18
Local Tunnel Operation Center					T19
Ventilation Stations for Smoke Extraction Systems					T20

» Tableau 8: Catégorisation des tunnels

System	Span / Height	Material	Superstructure Section	Type No.
Statical Determined	Small	Concrete	Solid	B01
		Prestressed Concrete	Solid	B02
		Composite / Steel	Hollow	B03
Statical Undetermined	Moderate	Concrete	Solid	B04
		Prestressed Concrete	Solid	B05
		Composite / Steel	Solid	B06
			Truss	B07
	Large	Prestressed Concrete	Hollow	B08
			Solid	B09
		Composite / Steel	Hollow	B10
			Solid	B11
			Truss	B12
Suspended / Cable-stayed	Large	Prestressed Concrete	Hollow	B13
			Solid	B14
		Composite / Steel	Hollow	B15
			Solid	B16
Earth Covered	Small	Steel	-	B17
		Concrete	-	B18
Moveable	Moderate	-		B19

» Tableau 9 : Catégorisation des ponts

2.3.2 Ponts

Le tableau 9 présente la catégorisation des ponts en fonction des 4 critères suivants :

» Système statique
» Portée ou hauteur
» Matériaux de construction
» Section transversale du tablier.

En prenant en compte le type particulier des ponts mobiles, un total de 19 types de ponts est établi.

2.4 Analyse de la vulnérabilité

Dans le cadre de la procédure d'évaluation de l'étape 2, le manuel fournit à l'utilisateur un ensemble de fiches utilisateurs (voir annexes) où pour chaque type d'objet, des valeurs par défaut de la vulnérabilité sont indiquées. En correspondance avec les tableaux de catégorisation 8 et 9, des fiches détaillées sont disponibles pour chaque type de pont et tunnel. Ces fiches montrent la décomposition de la vulnérabilité obtenue en fonction des menaces considérées. De plus, pour chacun des types de menaces, les deux composantes (dommages potentiels, faisabilité de l'attaque) sont indiqués (voir tableau 10). Dans la pratique, l'utilisateur peut adapter les valeurs par défaut en fonction de chaque situation spécifique. En raison de la grande diversité de tunnels et de ponts, il est conseillé (si nécessaire) de modifier pour chaque objet à évaluer dans l'étude les dommages potentiels et la faisabilité de l'attaque.

» **Tableau 10: Fiche utilisateur classique pour l'évaluation/analyse de la vulnérabilité**

TUNNEL - Type No. T01

		Damage Potential	Feasibility of Attack						VULNERABILITY
			object specific knowledge	technical knowledge	acquisition of material	access & transport	trigger event	TOTAL	
Explosion	Small	0	0	1	1	0	1	3	0
	Medium	2	1	0	1	1	1	4	8
	Major	6	1	0	0	1	1	3	18
	BLEVE	12	1	0	1	0	1	3	36
Fire	Major (200 MW)	4	1	0	1	1	1	4	16
	Arson	0	0	0	0	0	0	0	0
Mech. Impact	Ramming	0	0	0	0	0	0	0	0
	Projectiles	0	0	0	0	0	0	0	0
Sabotage		0	0	0	0	0	0	0	0
Attack on T19									87
Attack on T20									96
									261

LEGEND		
	Damage Potential	Estimated out-of-service time (in months)
	Feasibility of Attack	0...step difficult to accomplish
		1...step easy to accomplish
	Vulnerability	Damage Potential x Feasibility of Attack

>>TUNNEL OVERVIEW<<

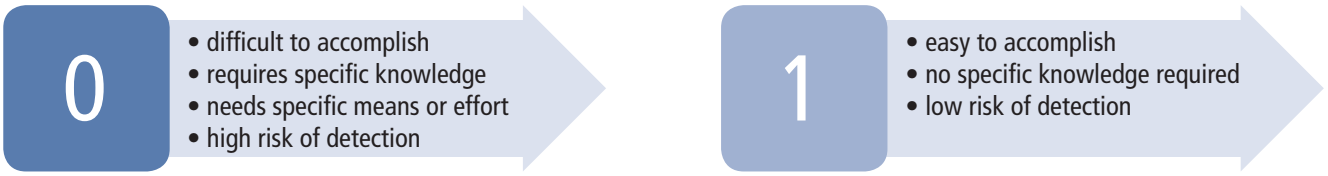
Pour adapter les fiches utilisateur, des informations sur le contexte des deux composantes de la vulnérabilité sont nécessaires. Dans les chapitres suivants, des données plus précises sont fournies sur la faisabilité d'une attaque et les dommages potentiels.

2.4.1 Faisabilité d'une attaque

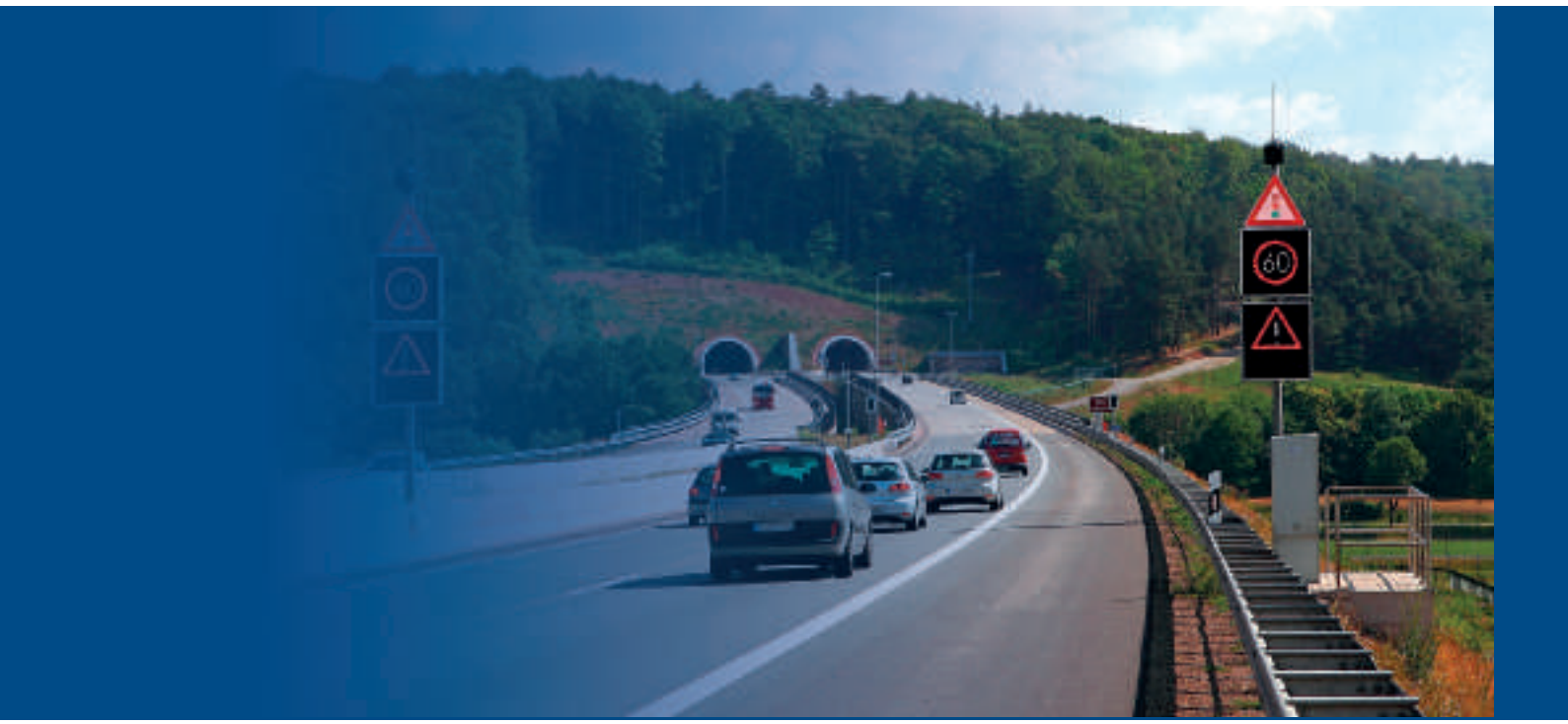
Pour réussir l'attaque d'un pont ou d'un tunnel, un attaquant doit pouvoir accomplir les 5 actions suivantes:

1. Acquérir des connaissances spécifiques de la structure : obtenir des connaissances techniques spécifiques de l'objet concerné, par exemples des points faibles du tunnel ou pont en lien avec une menace particulière.
2. Maîtriser la technologie : avoir des connaissances particulières des substances ou équipement à utiliser pour l'attaque, comme par exemple un certain niveau de connaissance en chimie pour produire du TNT ou de connaissances techniques pour construire un détonateur.
3. Acquérir des matériaux en quantités suffisantes : avoir la possibilité d'acheter des matériaux et équipements en quantités suffisantes pour être dangereux pour la structure spécifique à attaquer.
4. Avoir accès et pouvoir transporter des matériaux sur les parties vulnérables: premièrement, transporter les équipements/matériaux dangereux jusqu'à la structure sans être détecté. Deuxièmement, accéder aux parties vulnérables (points faibles) de l'objet, soit en termes de conception de la structure soit ceux des mesures de protection déjà mises en place.
5. Déclencher l'événement: avoir la capacité à déclencher l'événement à distance par le biais d'un système technologique ou bien avec l'intention de conduire une attaque suicide.

Pour chaque type de structure et menace, la probabilité que ces cinq actions puissent être accomplies avec succès peut être évaluée à l'aide d'une approche binaire simple, en attribuant à chaque action un « 0 » ou un « 1 » (schéma 11).



» Schéma 11 : Approche binaire pour l'évaluation de la faisabilité d'une attaque



2.4.2 Dommages potentiels

Comme évoqué dans l'introduction, le manuel se concentre d'abord sur la disponibilité des infrastructures de transport les plus importantes pour maintenir la fonctionnalité des principales voies de circulation. Ainsi, le critère pertinent pour l'évaluation des dommages potentiels d'une attaque est la possibilité d'utiliser l'infrastructure de transport considérée. Donc, le paramètre premier pour mesurer les impacts d'une attaque n'est autre que la durée de la mise hors service d'une structure.

Ce paramètre mesure à la fois les dommages sur l'ouvrage résultant d'un scénario donné et le délai typique de reconstruction nécessaire (délai de réparation ou remplacement du bien endommagé) de manière intégrative.

Toutefois, cette valeur ne peut pas être considérée comme une prévision du délai de reconstruction réel d'une structure spécifique, car celui-ci pourra varier en fonction de paramètres locaux et individuels. La valeur maximale a été fixée à 36 mois. Le délai de reconstruction comprend aussi le remplacement des équipements (ex. pour un tunnel : une attaque peut détruire l'équipement mais ne pas affecter la structure), la réparation des déformations (ex. pour les ponts, en cas d'absence d'effondrement de la structure).

2.4.3 Résultat

L'évaluation de la vulnérabilité s'effectue au niveau de l'objet. En d'autres termes, elle doit être répétée pour chaque objet de l'étude. L'utilisateur peut choisir d'utiliser les valeurs par défaut ou de les modifier pour le pont ou tunnel donné. Pour cela, la durée de la mise hors-service et/ou la difficulté à accomplir les cinq actions pour réussir une attaque peuvent être adaptées pour des types de menace personnalisés.

A partir de la valeur de vulnérabilité obtenue, les objets d'une partie du réseau peuvent être classés selon leur vulnérabilité vis-à-vis d'un ensemble de menaces. Ces informations sont importantes pour les prises de décisions de l'étape 3.

2.5 Autres recommandations

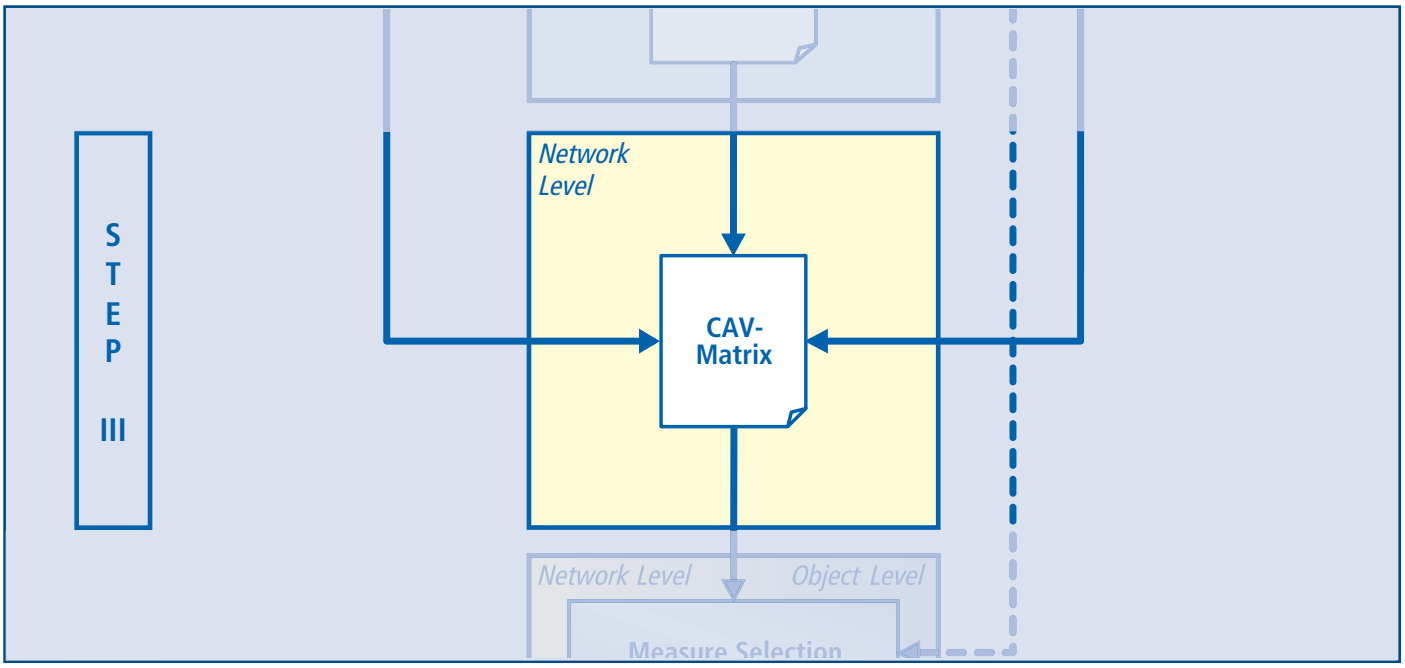
L'analyse de la vulnérabilité de l'étape 2 est une approche simplifiée permettant d'identifier les objets les plus vulnérables d'un réseau. Pour une évaluation plus détaillée des infrastructures les plus vulnérables, il est conseillé d'effectuer une analyse des risques au niveau de l'objet. Pour évaluer les dommages potentiels sur des structures particulières, des outils de simulation d'incendies, d'explosions ou d'impacts peuvent être utilisés. Dans le cadre des projets de recherche SeRoN (http://www.seron-project.eu) et SKRIBT (http://www.skribt.org), différents types d'analyses détaillées ont été réalisés. Plus d'informations sont disponibles sur les sites Internet respectifs et dans les rapports publiés.

3. Etape 3

3.1 Introduction

L'étape 3 est une procédure simple à l'échelle du réseau combinant tous les résultats des étapes précédentes dans une matrice CAV (Criticité, Attractivité, Vulnérabilité) et ayant pour objectif de trier ou classer les objets en fonction de trois paramètres et de faciliter les prises de décisions en matière de sûreté. A ce stade de la procédure, des aspects stratégiques entrent en jeu: la méthodologie produit une liste structurée des objets plus ou moins critiques, attractifs ou vulnérable, mais ne les classe pas sans ambiguïté. Pour y parvenir, l'utilisateur doit définir des priorités pour les paramètres de sécurité individuels ou ajouter d'autres aspects nécessaires aux prises de décisions.

Il est possible de sauter cette étape si seulement des objets individuels sont à évaluer à partir de leur vulnérabilité. La matrice CAV est une donnée essentielle pour les mesures de l'étape 4.



» Schéma 12 – Etape 3 (Matrice CAV)

3.2 Méthodologie

Dans le détail, les données d'entrée de la matrice sont les suivantes :

» Etape 1A : Criticité (à l'échelle du réseau)
» Etape 1B : Attractivité (à l'échelle de l'objet)
» Etape 2 : Vulnérabilité (à l'échelle de l'objet)

Les trois paramètres de la matrice CAV sont résumés dans un tableau selon le schéma 13. Dans les colonnes de gauche, les sections du réseau routier sont indiquées avec leur niveau critique. Sur chaque section se trouvent un certain nombre d'objets (tunnels et/ou ponts) avec les valeurs d'attractivité et de vulnérabilité correspondantes.

Network Level		*Object Level*		
Section No.	**STEP 1A Criticality**	**Object No.**	**STEP 1B Attractiveness**	**STEP 2 Vulnerability**
Sec_1	$Criticality_1$	Obj_{1_1}	$Attractiveness_{1_1}$	$Vulnerability_{1_1}$
		Obj_{1_2}	$Attractiveness_{1_2}$	$Vulnerability_{1_2}$
		...	...	...
		Obj_{1_m}	$Attractiveness_{1_m}$	$Vulnerability_{1_m}$
Sec_2	$Criticality_2$	Obj_{2_1}	$Attractiveness_{2_1}$	$Vulnerability_{2_1}$
		...	...	...
...	...	...	...	...
Sec_n	$Criticality_n$	Obj_{n_1}	$Attractiveness_{n_1}$	$Vulnerability_{n_1}$

» **Schéma 13: Matrice CAV (représentation abstraite)**

En principe, la matrice résume tous les résultats afin de permettre un classement des différents paramètres CAV en fonction des besoins de l'utilisateur. Après l'entrée de toutes les valeurs des trois paramètres CAV, l'utilisateur peut trier les objets dans la matrice à partir des priorités données dans chaque colonne. L'importance des paramètres CAV dépend des besoins de l'utilisateur.
Cette méthode ne définit pas de priorité pour les trois paramètres CAV mais permet de classer les infrastructures. Si l'objectif stratégique est la disponibilité du réseau routier, une approche possible peut être d'évaluer les objets sur les sections les plus critiques. Toutefois, d'autres approches sont aussi possibles en fonction de chaque problème individuel.

Sur le site Internet de SecMan, un outil logiciel simple peut être téléchargé comme aide à la mise en œuvre de la matrice CAV, et au classement des sections et des objets en fonction des priorités définies. **(Voir http://www.secman-project.eu)**.

Au final, la matrice permet à l'utilisateur :
» De répondre à la question : quel est la section ou l'objet le plus critique dans le réseau (et quelles sont les raisons de ce résultat), et

» De prendre plus facilement des décisions sur les objets et les sections sur lesquels des mesures sont à mettre en place en priorité.

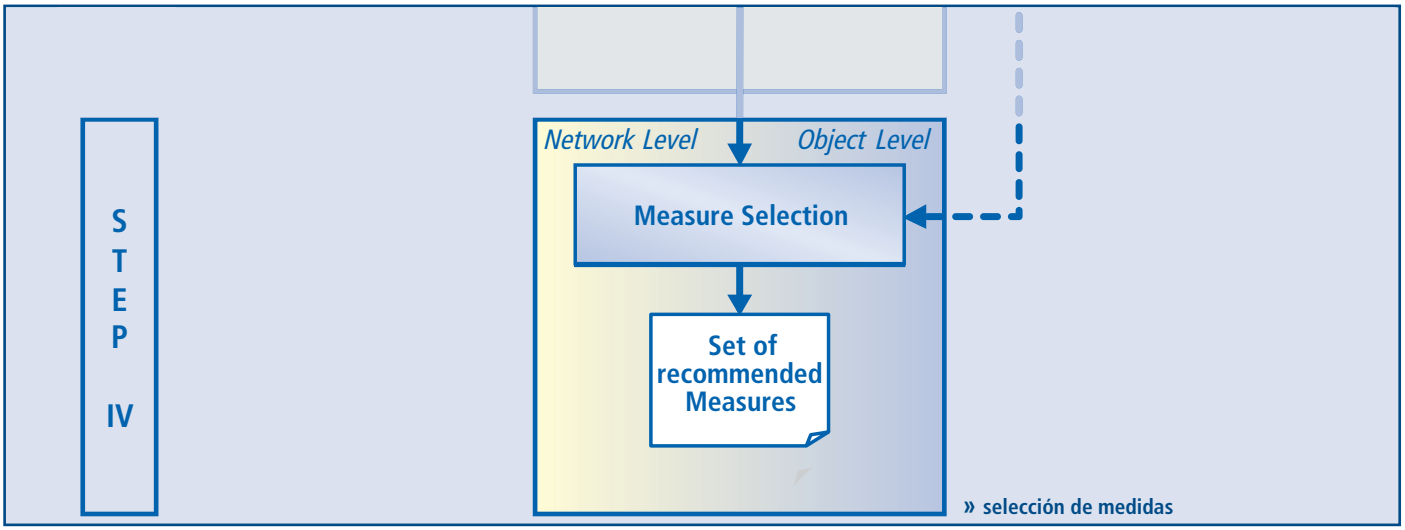
4. Etape 4

4.1 Introduction

De manière générale, l'objectif du processus de sélection des mesures est de présenter à l'utilisateur une aide dans le choix des mesures à prendre pour les structures ou sections de réseau définis comme prioritaires au cours de l'étape précédente. Le processus est automatisé pour permettre à l'utilisateur d'appliquer différentes mesures et de les tester de manière répétitive. Pour augmenter l'efficacité et la transparence de ce processus répétitif, un logiciel simple mais efficace a été mis en place. Dans la suite, des descriptions générales et des définitions sont données. Plus de détails et d'informations sur le contexte sont disponibles dans le mode d'emploi du logiciel de sélection des mesures téléchargeable avec le logiciel lui-même sur : **http://www.secman-project.eu.**

Il est important de comprendre que le processus de sélection des mesures donne une première indication sur des mesures de sûreté possibles. Les résultats obtenus doivent être comparés et confrontés aux données spécifiques des objets et du réseau pouvant influencer les risques et l'efficacité des contre-mesures mais qui ne sont pas compris dans les étapes 1, 2 et 3.

De plus, comme indiqué précédemment, l'utilisateur doit faire clairement la différence entre les mesures de sécurité et de sûreté. Actuellement, un grand nombre de mesures de sécurité sont déjà prises en compte dans les phases de conception et d'opération des objets et réseaux évalués. Avec les analyses détaillées, qui ne font pas partie de ce manuel, il est possible d'évaluer quelles mesures de sécurité existantes ont un impact sur la sûreté générale du réseau ou de l'objet. Les mesures de sûreté ont un effet positif sur la sécurité globale mais ce sujet dépasse le champ d'application de ce manuel.



» Schéma 14: Catégorisation des mesures

4.2 Catégorisation des mesures

Dans le manuel, les mesures sont regroupées en fonction du tableau suivant.

Type de mesure		Description
Mesures au niveau du réseau		Les mesures au niveau du réseau s'appliquent à toute la partie du réseau prise en considération. En d'autres termes, ces mesures sont mises en place pour des parties complètes du réseau routier et non sur les différents objets de ce dernier. La sélection des mesures n'est pas influencée par les variations des caractéristiques de la partie du réseau. De plus, les mesures du réseau sont efficaces pour limiter la criticité et la faisabilité d'une attaque.
Mesures générales au niveau de l'objet		Les mesures générales au niveau de l'objet concernent toutes les mesures applicables à tous les objets (ponts, tunnels et infrastructures associées). Les mesures générales sont efficaces pour limiter la criticité et la faisabilité d'une attaque.
Mesures pour les ponts	**Tous les ponts**	Mesures à l'échelle de l'objet s'appliquant à tous les ponts.
	Différents types de ponts	Mesures à l'échelle de l'objet s'appliquant à certains types de ponts, les types étant définis à l'étape 2.
Mesures pour les tunnels	**Tous les tunnels**	Mesures à l'échelle de l'objet s'appliquant à tous les tunnels.
	Différents types de tunnels	Les mesures à l'échelle de l'objet s'appliquant à certains types de tunnels les types étant définis à l'étape 2.
Mesures pour les infrastructures associées		Trois types d'objets supplémentaires sont ajoutés : centres opérationnels et de contrôle, installations de ventilation pour système d'extraction des fumées, autres objets et éléments électrotechniques.

» Schéma 14: Catégorisation des mesures

Pour chaque groupe, un ensemble de mesures par défaut est proposé dans le manuel. La méthode permet d'adapter l'ensemble des mesures en ajoutant ou supprimant certaines d'entre-elles.

4.3 Processus de sélection des mesures

La méthodologie du processus de sélection des mesures permet à l'utilisateur de déterminer les mesures pertinentes pour chaque type de structure et pour chaque menace, et de les combiner dans un catalogue de mesures. De plus, rappelons que ce processus peut être utilisé individuellement, indépendamment des autres étapes, comme première indication des stratégies possibles en matière de sécurité.

Par ailleurs, l'utilisateur peut ajouter, supprimer ou modifier les mesures. Cependant, les réglementations applicables, les approches techniques, les considérations sociales et politiques ainsi que les régimes juridiques du pays de l'étude devront être pris en considération. Lors de l'ajout d'une nouvelle mesure, l'utilisateur doit aussi définir un lien (un effet) entre la nouvelle mesure et les paramètres CAV (discutés à l'étape 3).

Pour disposer de la liste de mesures la plus adaptée au problème particulier, il est recommandé à l'utilisateur de choisir des paramètres pertinents. Dans le logiciel, trois différents groupes de paramètres sont proposés.

Type de mesure :

Tout d'abord, l'utilisateur peut sélectionner des mesures en fonction du type d'objet ou de la section de réseau. Comme expliqué au point 4.2, les mesures sont catégorisées en cinq groupes. Le processus de sélection permet d'adapter la requête en fonction d'un problème spécifique. Ceci permet à l'utilisateur de choisir entre les mesures à l'échelle du réseau et celles au niveau de l'objet. Il est aussi possible d'opter pour tous ou seulement un type d'objet en particulier.

Nouvel objet ou rééquipement :

Certaines mesures ne s'appliquent qu'aux nouveaux objets, d'autres seulement aux structures existantes. Dans ce groupe de paramètres, l'utilisateur peut choisir si l'objet analysé n'est pas encore construit (nouvel objet/nouveau réseau) ou si les mesures doivent être inclues dans un cycle de rééquipement.

Paramètres CAV :

En sélectionnant des paramètres CAV individuels, la méthode permet d'obtenir les effets des mesures en fonction de la criticité d'une section de réseau ou de l'objet, des dommages potentiels et de la faisabilité de l'attaque. Toutefois il est conseillé de sélectionner pour la première itération du processus de sélection, dans un premier temps tous les paramètres puis dans un deuxième temps de réduire leur nombre.

4.4: Autres recommandations

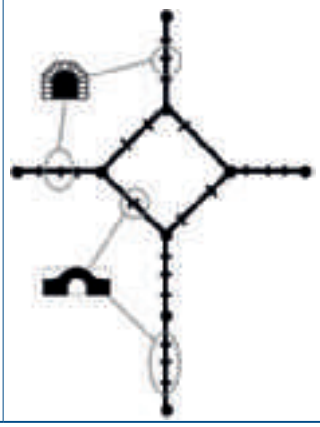
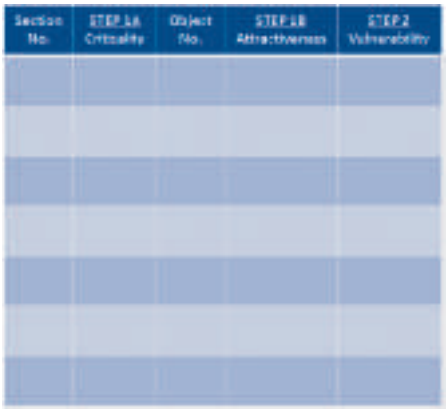
Le processus de sélection des mesures est défini sur la base des propriétés communes, des caractéristiques et particularités des objets/réseaux de manière automatique et répétée pour différents réseaux, ponts, tunnels et infrastructures associées. L'avantage de cette approche est que le processus de sélection des mesures peut être effectué pour un grand nombre d'objets ou réseau avec les mêmes procédures et définitions. Cependant, tous les détails et caractéristiques des objets/réseaux n'ont pas pu être inclus dans la méthodologie. Il est donc indispensable de réétudier de manière critique les effets des mesures. Pour cette révision, on pourra s'aider des questions suivantes :

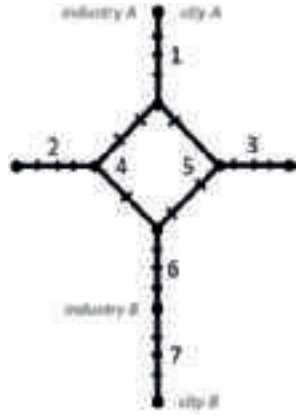
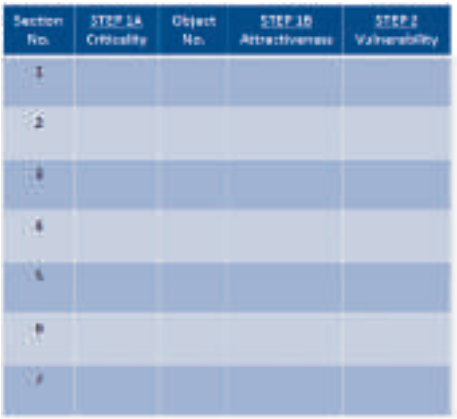
- Les mesures sont-elles efficaces pour l'objet/le réseau étudié?
- Les coûts des mesures sont-ils justifiés?
- Les mesures couvrent-elles les risques identifiés?
- La mise en place des mesures s'accompagne-t-elle d'effets négatifs?
- Le niveau de sécurité est-il réduit avec ces mesures?
- L'impact général de la combinaison de mesures et de la prise de décision est-il correct?
- La combinaison des paramètres de sélection des mesures est-elle adaptée et couvre-elle toutes les menaces principales?
- Les mesures et leurs effets sont-ils correctement définis ? Reflètent-ils les propriétés de l'objet réel?

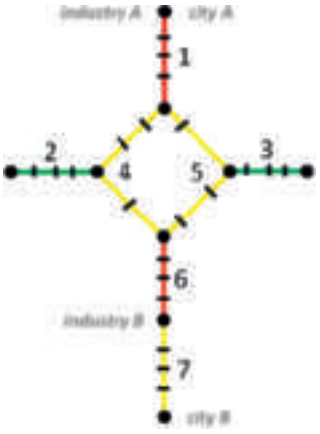
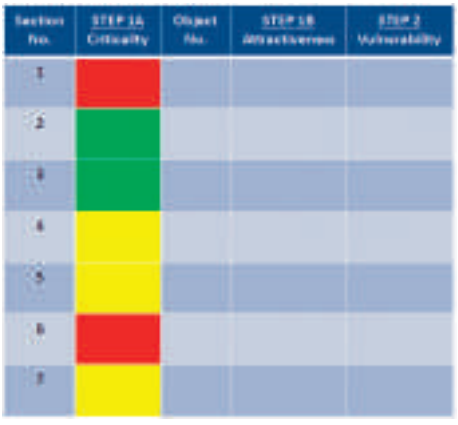
Pour répondre à toutes ces questions, des analyses supplémentaires détaillées (niveau 2) sont nécessaires. Celles-ci pourraient comprendre notamment une analyse détaillée des risques avec et sans les mesures pour obtenir des informations sur l'efficacité d'une mesure. De plus, une analyse de la rentabilité (coûts/bénéfices) pourra s'avérer utile. Des échanges sur l'applicabilité et sur la méthode pour ces analyses complémentaires ont été présentés dans le cadre des différents projets de recherche menés par SeRoN **(http://www.seron-project.eu)** et SKRIBT **(http://www.skribt.org)**.

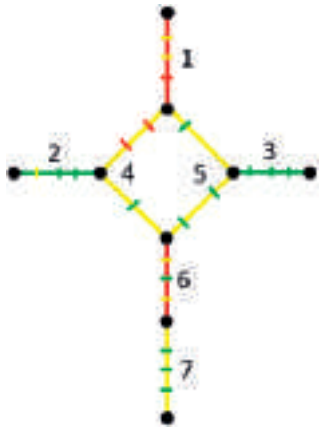
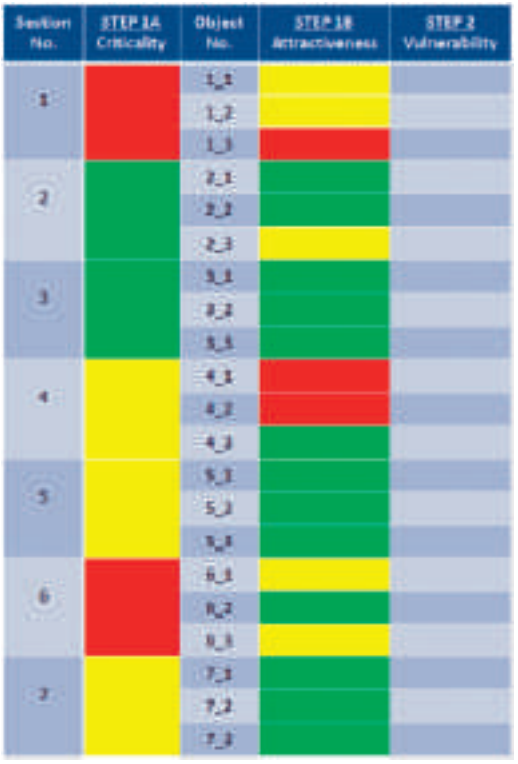
TROISIÈME PARTIE 3: Exemple pratique

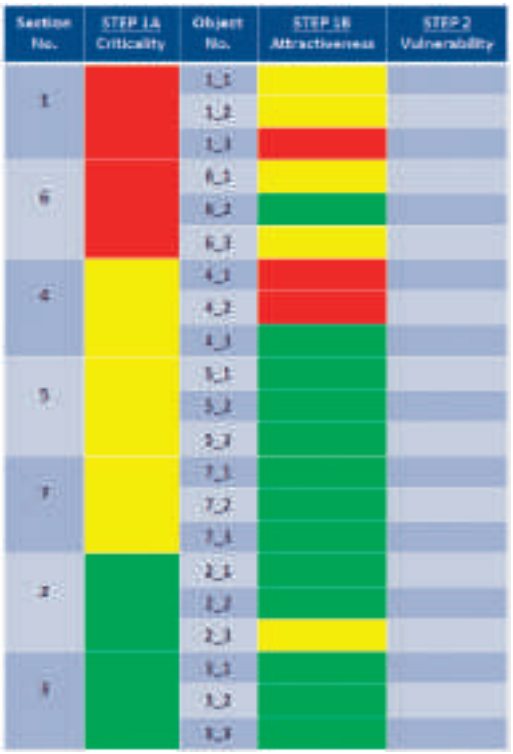
L'exemple pratique suivant illustre la méthodologie sur une partie très simple d'un réseau. Cet exemple devrait aider l'utilisateur à suivre la procédure en 4 étapes. Toutefois, cet exemple reste très limité. La mise en œuvre réelle dans le cas de l'utilisateur pourra être différente en termes de champ d'application et de résultats.

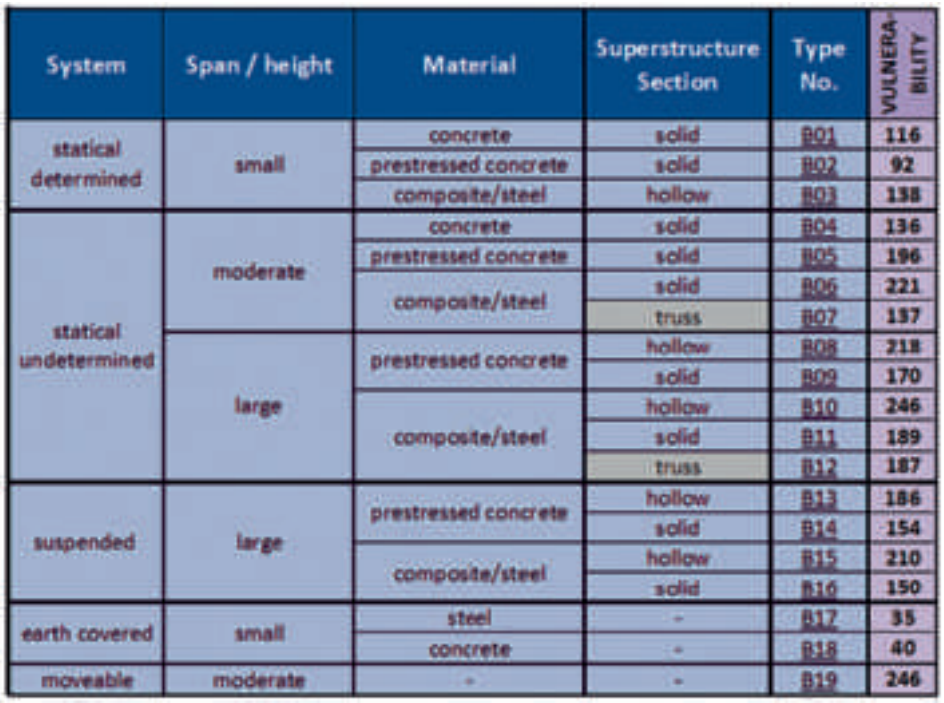
	Réseau	Matrice CAV	Commentaires
1			Au début, il convient de définir la partie du réseau à évaluer et de fixer les limites de l'étude de cas. Sur la partie du réseau étudiée se trouvent plusieurs tunnels et ponts. Dans l'exemple proposé, ils sont au nombre de 21. Pour les étapes suivantes, certaines informations sur le trafic et les données de base sur la partie du réseau étudiée et ses objets sont nécessaires. Nous supposons que ces données générales sont disponibles auprès des utilisateurs de ce manuel.

	Réseau	Matrice CAV	Commentaires
2			A partir des jonctions principales sur le réseau de transport, la partie de réseau étudiée est divisée en 7 sections numérotées. Les critères de définition des sections dépendent de l'utilisateur mais il est recommandé d'utiliser les mêmes paramètres de trafic que pour le niveau 1A, évaluation de la criticité. Dans l'exemple, deux villes et deux zones industrielles au nord et au sud sont raccordées par une route principale. La liaison entre les deux se divise en deux routes équivalentes.

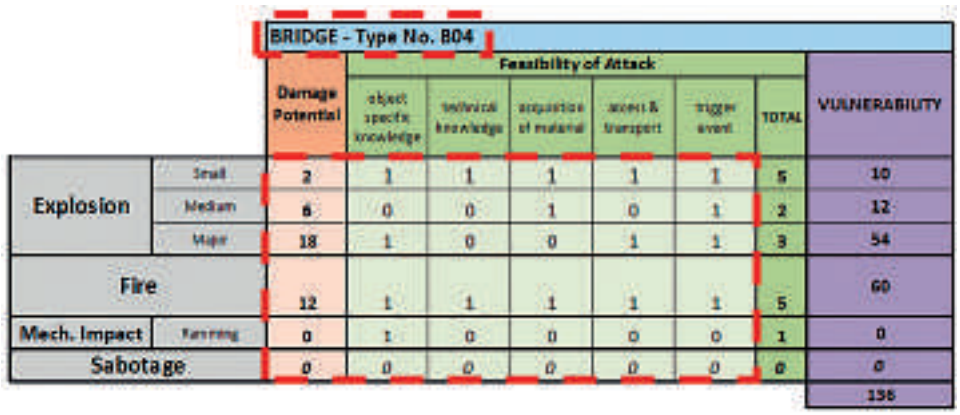
	Réseau	Matrice CAV	Commentaires
3			Chaque section est évaluée d'un point de vue qualitatif à partir des paramètres de trafic comme les itinéraires de contournement, le trafic moyen journalier annuel (TMJA), la proportion de poids lourds dans le trafic et l'aptitude à accueillir des transports spéciaux. Les sections sont classifiées « très critiques », « critiques » ou « moins critiques ». Dans l'exemple, le lien nord-sud est une route très critique en raison d'un trafic moyen journalier annuel élevé, d'une large proportion de poids lourds entre la ville A et B ainsi que de l'absence de voies de contournement. Dans les sections 4, 5 et 7, la criticité est plus faible du fait (a) de l'existence d'un itinéraire de contournement pour les sections 4 et 5 et (b) de la part moins importante de poids lourds dans le trafic de la section 7. Les sections 2 et 3 ne sont pas sur l'axe principal de transit et sont moins importantes pour le trafic.

	Réseau	Matrice CAV	Commentaires
4			A l'étape 1B, l'évaluation de l'attractivité est réalisée pour tous les objets de la partie du réseau étudiée, à partir de paramètres comme la valeur symbolique, le nombre potentiellement élevé de décès ou d'autres effets secondaires en cas d'attaques sur les infrastructures. Les objets sont soit « très attractifs », « attractifs » ou « peu attractifs ». Dans l'exemple, la plupart des objets sont peu attractifs à l'exception de certain tunnels et ponts connus à l'échelle internationale (ex : pont historique important pour le paysage urbain, tunnel sur une route de vacances connu pour ses bouchons l'été, etc…) Ces objets sont évalués avec un niveau d'attractivité différent

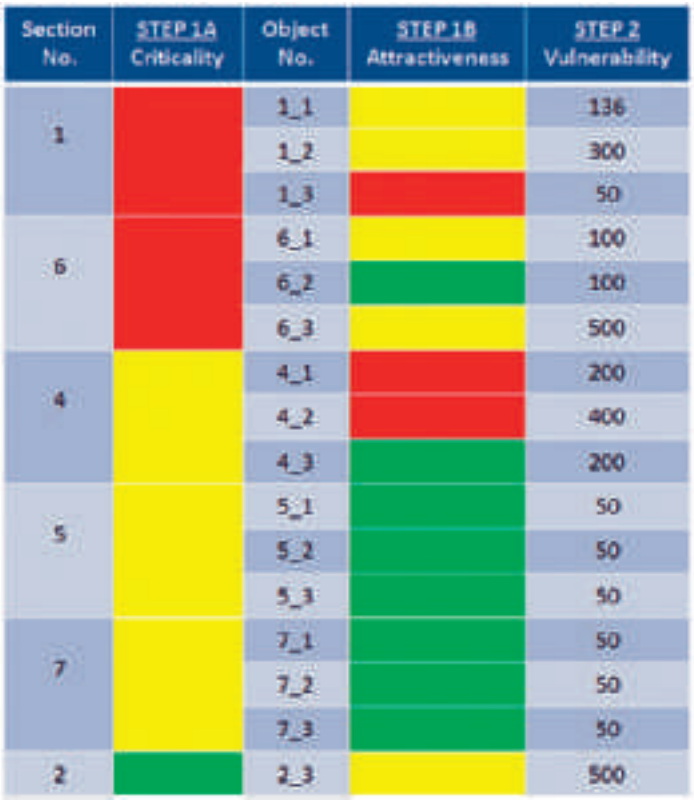
	Réseau	Matrice CAV	Commentaires
5			Comme déjà indiqué, l'étape 1 peut être utilisée comme méthode de présélection afin de réduire le nombre d'objets à évaluer au cours des étapes suivantes. En fonction de ses priorités individuelles, l'utilisateur doit définir les objets à évaluer dans l'étape 2. La matrice CAV permet à l'utilisateur de classer les sections et les objets en fonction de la priorité fixée. Dans l'exemple, la priorité numéro 1 est donnée à la criticité, suivie par l'attractivité. En fonction de quoi, il a été décidé que les sections très critiques et critiques ainsi que les objets très attractifs et attractifs seront analysés plus avant. Il en résulte une analyse plus détaillée de la vulnérabilité à mener pour 16 objets.

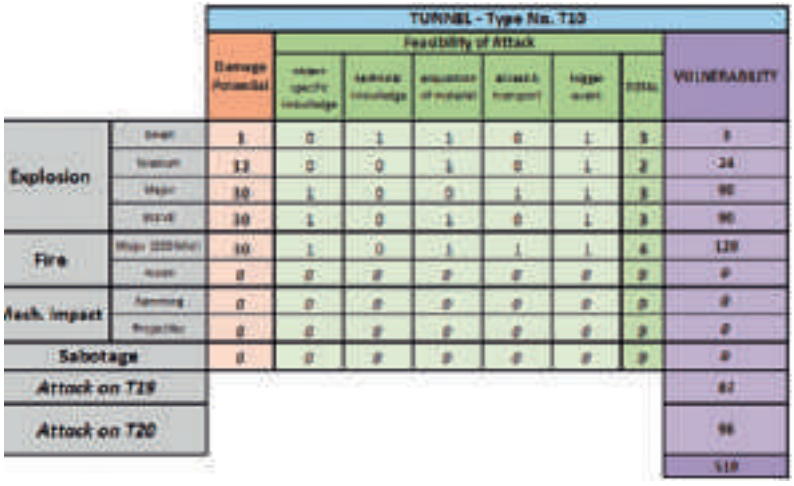
	Matrice CAV	Commentaires
6		Dans le cadre de l'évaluation de la vulnérabilité de l'étape 2, le tableau général (disponible pour les tunnels et les ponts) est utilisé pour catégoriser les objets. Le tableau comprend des valeurs par défaut valables pour des ponts et tunnels communs sans caractéristiques particulières. En commençant par le premier objet de la matrice, l'objet 1_1 est un pont dont la structure est hyperstatique, construit en béton et avec tablier massif. D'après la catégorisation de SecMan, il s'agit d'un pont de type B04 avec une valeur de vulnérabilité par défaut de 136.

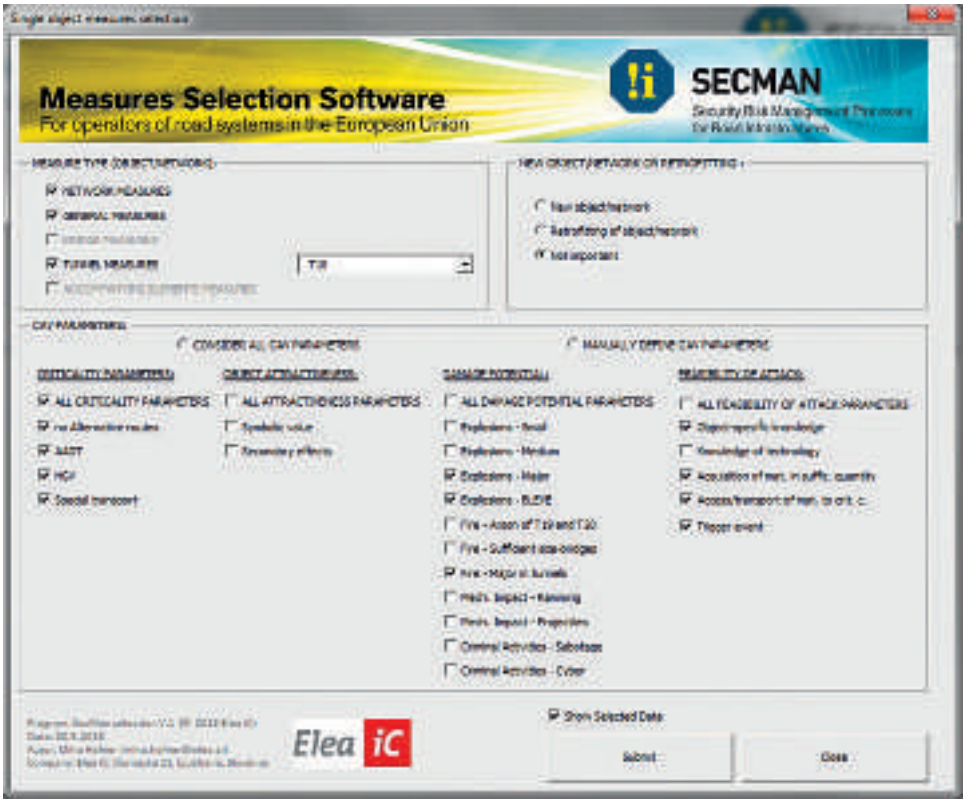
System	Span / height	Material	Superstructure Section	Type No.	VULNERABILITY
statical determined	small	concrete	solid	B01	116
		prestressed concrete	solid	B02	92
		composite/steel	hollow	B03	138
statical undetermined	moderate	concrete	solid	B04	136
		prestressed concrete	solid	B05	196
		composite/steel	solid	B06	221
			truss	B07	137
	large	prestressed concrete	hollow	B08	218
			solid	B09	170
		composite/steel	hollow	B10	246
			solid	B11	189
			truss	B12	187
suspended	large	prestressed concrete	hollow	B13	186
			solid	B14	154
		composite/steel	hollow	B15	210
			solid	B16	150
earth covered	small	steel	-	B17	35
		concrete	-	B18	40
moveable	moderate	-	-	B19	246

	Matrice CAV	Commentaires
7		Le manuel donne la possibilité à l'utilisateur d'ajuster les dommages potentiels de et/ou la faisabilité d'une attaque en fonction des propriétés spécifiques du pont évalué. Les ajustements peuvent notamment se faire dans les cas suivants : » Des mesures de protection existent déjà (protection contre l'explosion) → Réduit le risque de dommages » Accès difficile à un pont en raison des conditions topographiques → accès & transport = 0 pour toutes les menaces » etc. Il est conseillé d'effectuer les ajustements pour chaque objet de l'étude. Toutefois, ce n'est pas un prérequis dans la mesure où la méthode peut également être appliquée avec des valeurs par défaut.

BRIDGE - Type No. B04			Feasibility of Attack						
		Damage Potential	object specific knowledge	technical knowledge	acquisition of material	access & transport	trigger event	TOTAL	VULNERABILITY
Explosion	Small	2	1	1	1	1	1	5	10
	Medium	6	0	0	1	0	1	2	12
	Major	18	1	0	0	1	1	3	54
Fire		12	1	1	1	1	1	5	60
Mech. Impact	Ramming	0	1	0	0	0	0	1	0
Sabotage		0	0	0	0	0	0	0	0
									135

	Matrice CAV	Commentaires
8		Après avoir répété l'étape 2 et évalué la vulnérabilité pour tous les objets considérés comme prioritaires, les résultats peuvent être saisis dans la matrice CAV. Remarque : Comme des ajustements peuvent être effectués par l'utilisateur, deux objets du même type peuvent avoir des vulnérabilités différentes. Les étapes 1 et 2 sont désormais terminées, et la matrice CAV est complète. L'action principale de l'étape 3 est de fixer la priorité à donner aux trois paramètres CAV respectifs. En fonction des priorités arrêtées par l'utilisateur, le classement des objets peut être très différent. L'exemple suivant montre qu'en attribuant des priorités différentes, trois objets différents peuvent être classés en premier : » 1. Criticité, 2. Attractivité: objet 1_3 » 1. Criticité, 2. Vulnérabilité: objet 6_3 » 1. Attractivité, 2. Vulnérabilité: objet 4_2 Il incombe à l'utilisateur de définir la priorité des paramètres CAV en fonction de ses objectifs stratégiques. Ce classement final obtenu peut être utilisé comme entrée pour l'étape 4 ou pour identifier des objets à soumettre à des évaluations complémentaires (par ex. analyse détaillée des risques).

	Matrice CAV	Commentaires
9		Le résultat du processus de prise de décision de l'étape 3 est une liste (restreinte) d'objets classés selon leur priorité pour des mesures à mettre œuvre. Dans l'exemple, la première priorité est la criticité puis vient la vulnérabilité. C'est pourquoi le premier objet du classement est l'objet 6_3 qui se trouve sur une section de réseau très critique et affiche une vulnérabilité de 510. Pour réduire le risque de sûreté général, il est nécessaire d'identifier les mesures permettant de diminuer la criticité et la vulnérabilité. La fiche détaillée sur la vulnérabilité de l'objet considéré est utilisée pour appréhender les menaces présentant les plus gros dommages potentiels (explosion majeure, BLEVE et gros incendie) et les paramètres critiques pour la faisabilité d'une attaque. L'étape suivante consiste à identifier les mesures à mettre en œuvre pour réduire les dommages potentiels et les paramètres de la faisabilité d'une attaque.

	Matrice CAV	Commentaires
10		Le logiciel de sélection des mesures aide l'utilisateur à identifier les mesures appropriées pour l'objet considéré à partir des priorités définies. Dans le logiciel, le processus de sélection des mesures démarre et les options suivantes sont vérifiées : » Mesures réseau au niveau du réseau » Mesures générales et mesures spécifiques à l'échelle de l'objet - type de tunnel T10 » Mesures pour tous les paramètres critiques » Mesures pour les paramètres de dommages potentiels spécifiques » Mesures pour les paramètres de la faisabilité d'une attaque. Après avoir soumis la requête, le logiciel liste un ensemble de 21 mesures recommandées. Pour chaque mesure, une fiche technique contenant les informations détaillées est disponible en annexe. A partir de cette liste, l'utilisateur peut définir les mesures à mettre en œuvre pour l'objet considéré dans son cas particulier.

QUATRIÈME PARTIE: Liste des mesures

MESURES AU NIVEAU DU RESEAU:

N.01 Redondance du réseau (logistique, informations, plans en cas de déviation, équipements et infrastructures
Network, section traffic redundancy

La redondance du réseau est une mesure avec un très grand champ d'application. Dans le cas où certains objets doivent être fermés sur une section du réseau, une possibilité de circulation sur un réseau de transport parallèle à proximité est mise à disposition. Trois types de redondance sont proposés :

- Redondance fournie par un réseau de routes parallèles au même niveau,
- Redondance fournie par un réseau de routes parallèles de niveau supérieur/inférieur,
- Redondance fournie par un réseau de routes parallèles avec d'autres moyens de transport afin d'assurer une capacité de transport minimale.

Il convient de souligner que la redondance du réseau doit être mise en œuvre pour une période limitée dans le temps et avec des aspects logistiques, des équipements, infrastructures et plans de contournement prédéfinis.

N.02 Protection des informations sensibles liées à l'importance du réseau
Protection of sensitive information related to network importance

Les effets secondaires indésirables d'une clôture non prévue d'une section de réseau peuvent être importants. Il est fortement déconseillé de dévoiler ces effets à des personnes non autorisées ou au grand public. Dès lors, la préparation d'une stratégie pour la protection de ces données est nécessaire. Il est indispensable d'assurer des échanges réguliers entre les différents autorités et services.

De manière générale, les informations sur l'attractivité d'un objet, notamment sur la valeur symbolique, sont connues du public. Les effets secondaires sont moins connus pour un grand nombre de réseaux même pour les propriétaires des infrastructures et les autorités. Si le public dispose d'informations sur les effets secondaires, cela pourra augmenter le niveau d'attractivité du réseau. Les informations sur les effets secondaires peuvent être:

- L'impact économique
- Les dommages pour la société
- Etc.

N.03 Formation, entrainement et exercices en cas d'attaque (au niveau du réseau)
Education, training and exercises for the cases of the attack (network level)

La formation, l'entrainement et les exercices au niveau du réseau sont des mesures très importantes à mettre en place dans de nombreux groupes:

- Usagers de l'infrastructure : la mission principale est de guider les utilisateurs en dehors de la zone affectée pour assurer le travail sans encombre des services de secours.
- Eléments en danger (effets secondaires potentiels…), si identifiés : Chaque effet secondaire a ses propres caractéristiques. La formation, l'entrainement ainsi que les exercices doivent être organisés en conséquence. La mise en place de plans d'urgence pour plusieurs incidents peut être très efficace.
- Formation, entrainement et exercices s'adressant aux personnels du centre de contrôle et des équipes de secours.
- Formation, entrainement et exercices des exploitants et propriétaires.

Il est important de noter que ces mesures peuvent avoir des impacts négatifs car le grand public prend conscience des points sensibles de l'objet, de la structure ou du réseau.

N.04	**Plans d'actions en cas de détection d'une attaque ou d'activités suspectes** **Contingency plan for the case of the attack**

Après avoir évalué le risque de sûreté, l'utilisateur doit pouvoir prédire ou décider

» Quelles sont les menaces qui peuvent être contrôlées

» Quelles sont les conséquences potentielles pertinentes à limiter.

Ces deux questions concernent les caractéristiques des parties du réseau, sections et objets critiques. Les mesures doivent donc être ciblées en fonction. Cela devra aussi guider l'organisation des interventions et des responsabilités pour les plans d'action. Si l'analyse des menaces détectées et des moyens déjà organisés révèle une efficacité insuffisante, les deux étapes suivantes peuvent être ajoutées:

» Des moyens supplémentaires peuvent être mobilisés, entraînés, formés, et ajoutés aux équipes d'intervention.

» Les moyens existants peuvent être équipés, formés et entraînés.

De cette manière, l'opérateur de l'infrastructure n'est pas pris au dépourvu si l'une des menaces identifiées se matérialise. De plus, les systèmes automatiques doivent répondre de façon adaptée dans un certain nombre de cas comme en cas d'attaques multiples, d'informations confuses, d'événements non prévus, de manque d'information, etc...

N.05	**Contrôles, interventions, patrouilles ou présence de la police (ou d'autres services de sécurité), sur des sections ou réseaux critiques. Police and security services control of the section/network**

S'ils sont considérés comme critiques, des réseaux entiers ou des sections de réseau sont contrôlés et surveillés par la police, les services de sécurité, etc…Cela peut être fait par le biais de surveillance par hélicoptère, de patrouilles, de présence physique…dans ou à proximité des installations vitales ou stratégiques.

MESURES GENERALES AU NIVEAU DE L'OBJET

GO.01	**Surveillance du centre de contrôle par rapport à des attaques et activités suspectes** **Control centre surveillance for the attacks and suspicious activities detection**

Le personnel du centre de contrôle dispose des informations nécessaires sur l'exposition au risque d'un objet (selon les responsabilités assignées). Le personnel sait comment réagir dans les différentes configurations d'attaques possibles. Pour contrôler ces événements et pour détecter des activités suspectes, les techniques suivantes peuvent être utilisées des questions de sûreté:

» CCTV pour la sûreté;

» Détecteurs de mouvement pour la sûreté;

» Détection/surveillance vidéo automatique pour la sûreté;

» Détection des matières dangereuses par radio-identification (RFID) pour la sûreté;

» Détection de la présence de gaz pour la sûreté.

Par ce biais, les objectifs de ces techniques qui ont pour objectif premier la sécurité sont aussi appliqués à la sûreté des objets ou du réseau. Il faut cependant souligner que toute mesure doit être ciblée en fonction des risques de sûreté évalués. Il est donc nécessaire de réévaluer et d'ajuster les équipements existants pour la sûreté et en vue de:

» La détection des événements critiques et/ou,

» La prévention des événements critiques et/ou,

» La maîtrise des événements critiques.

Pour cela, chaque objet, section ou réseau a donc besoin de son propre système de surveillance pour couvrir les risques identifiés et de son propre plan d'actions sous la forme d'un plan d'urgence ou équivalent.

GO.02 Formation, entrainement et exercices en cas d'attaque (à l'échelle de l'objet)
Education, training and exercises for the cases of the attack (object level)

La formation, l'entrainement et les exercices au niveau d'un objet sont des mesures importantes à mettre en place pour de nombreux groupes de personnes:

- Usagers de l'infrastructure : bien que la capacité à se secourir par soi-même soit du plus grand intérêt pour les usagers, ils n'ont le plus souvent pas conscience de la situation réelle et des risques potentiels en cas d'incident. La mission principale concernant les usagers est de les guider en dehors de la zone dangereuse et d'assurer le travail sans encombre des services d'urgence.
- Formation, entrainement et exercices s'adressant aux personnels du centre de contrôle et des équipes de secours.
- Formation, entrainement et exercices pour l'exploitant et le propriétaire.

Il est important de noter que ces mesures peuvent avoir des impacts négatifs car le grand public prend conscience des points sensibles de l'objet, de la structure ou du réseau.

GO.03 Prévention des approches et des accès non-autorisés (signalisation, clôtures, portes, barrières)
Access and approach prevention (signs, fences, doors, barriers)

Il s'agit de la mesure principale pour réduire la faisabilité d'une attaque. Différents types de mesures peuvent être conçues pour prévenir les risques identifiés:

- Panneaux signalétiques et ralentisseurs
- Clôtures et portes
- Barrières…

Ces mesures peuvent concerner les personnes, les voitures personnelles, les camions, les poids lourds…

La conception de ces mesures d'une manière qui attire l'attention peut avoir des effets négatifs (les éléments très protégés peuvent être très attractifs pour une attaque). Pour éviter cet effet, des mesures architecturales peuvent être nécessaires.

GO.04 Plans d'urgence contre les attaques d'origine humaine
Contingency plan for man-made attacks (object level)

Immédiatement après la détection d'une attaque ou d'activités suspectes, tous les services en charge et organisations impliquées doivent être informés. Les données nécessaires doivent être transmises conformément aux plans d'actions et d'urgence. Pour le moment, ces plans d'actions sont élaborés dans le cadre de l'organisation de la sécurité. Il est important de souligner que ces attaques sont des problèmes spécifiques qui combinent différents services, organisations, groupements d'intérêt divers avec les caractéristiques spécifiques d'un objet (vulnérabilité). Les systèmes d'alerte doivent les prendre tous en considération et les impliquer à la hauteur de leurs responsabilités.

GO.05 Mesures architecturales
Architectural measures

Les techniques architecturales suivantes peuvent utilisées:

- Zone de sécurité pour assurer la visibilité
- Barrières de sécurité et ralentisseurs pour maintenir la visibilité
- Eclairage adapté
- Profils larges pour les passages souterrains, les espaces ouverts devant les infrastructures
- Formes simples des objets, façades ; absence d'espace cachés, angles/coins…
- Combinaison de plusieurs objets dans une seule unité architecturale claire.
- Absence de formes spécifiques où poser des objets comme par exemple des rebords de fenêtres ou des étagères…
- Recouvrement total ou partiel des objets par de la terre
- Protection visuelle des zones d'exploitation et d'activité considérées sensibles comme le centre de contrôle.

Il est très important de mettre en œuvre ces mesures selon les risques de sûreté identifiés. Les mesures architecturales contribuent aussi à limiter l'attractivité. Les objets très protégés sont attractifs!

GO.06	**Protection de la documentation des objets et vulnérabilité des informations** **Protection of object documentation and vulnerability information**
L'évaluation des risques de sûreté fournit des informations qui ne doivent pas être divulguées à des personnes non autorisées ou au grand public. Certaines règles doivent donc être établies définissant leur utilisation et les personnes autorisées y ayant accès. De plus, toutes les données connexes, consignes et tous les plans en cas d'attaque doivent respecter ces mêmes principes de restriction.	
GO.07	**Services d'intelligence et activités anti-terroristes** **Intelligence services and antiterrorist activities**
Cette mesure peut influencer fortement les paramètres de faisabilité d'une attaque. Chaque pays dispose de son propre système légal et de sa propre organisation à ce sujet. Cette mesure doit être minutieusement étudiée et une coordination adaptée doit être assurée entre les autorités responsables et les services concernés.	
GO.08	**Contrôles, interventions, patrouilles ou présence de la police (ou d'autres services de sécurité) sur des objets critiques. Police and security services control of the object**
S'il est considéré comme critique, l'élément ou objet est contrôlé et surveillé par la police, les services de sécurité, etc…suivant le plan de sécurité. Cela peut être fait par le biais de patrouilles, de surveillance par hélicoptère, de présence physique etc. dans ou à proximité des endroits stratégiques.	

MESURES POUR LES PONTS

B.01	**Redondance du trafic pour les ponts** **Traffic redundancy for the bridge**
Cette mesure est efficace pour augmenter la capacité d'utilisation d'un pont après un incident présentant des dommages potentiels élevés. Elle est pertinente durant la phase de conception d'un nouvel objet. La redondance globale signifie qu'une moitié au moins du pont (dans un sens) est disponible pour le trafic après des travaux de maintenance mineurs suite à un événement. Deux approches sont possibles pour y parvenir: » Prévoir des tabliers séparés par un joint longitudinal. De cette manière, il est possible de réparer ou remplacer la partie endommagée du tablier sans perturber le trafic sur la partie non endommagée. » Etablir des sous-structures distinctes (tabliers sur des piliers séparés). De cette façon, il est possible non seulement de réparer ou remplacer la partie du tablier endommagé, mais aussi les piliers abîmés, pendant que le trafic circule sur la partie non-endommagée (sous-structure indépendante avec tablier). Dans les cas où la redondance d'un objet n'est pas faisable, la redondance au niveau du réseau est proposée pour les objets critiques, attractifs ou vulnérables.	
B.02	**Prévenir le stationnement sous le pont** **Parking under the bridge prevention**
Cette mesure peut réduire la possibilité de placer des explosifs ou matières inflammables sous un pont. De cette manière, il est possible de diminuer la faisabilité d'une attaque mais aussi les dommages potentiels des menaces correspondantes.	
B.03	**Prévenir le dépôt de déchets ou le stockage de matériaux sous le pont** **Preventing of waste material disposal or material storage under the bridge**
Les matières inflammables ou explosives entreposées sous un pont ou à proximité peuvent constituer une grande menace pour les ponts avec des culées relativement basses. En prévenant le dépôt de déchets ou autres matériaux sous un pont, il est possible de diminuer la faisabilité d'une attaque mais aussi les dommages potentiels des menaces correspondantes.	
B.04	**Barrières anti-explosion** **Explosion barriers**
Pour les ponts, les dégâts des explosions importantes peuvent être limités ou supprimés à l'aide de barrières anti-explosion (ex. digues).	
B.05	**Augmenter le gabarit et/ou la hauteur de sécurité** **Increase of clearance profile and/or safety height**
Si le gabarit et/ou la hauteur de sécurité est suffisant (culées hautes), les effets d' explosions et incendies importants peuvent être limités voire supprimés. Une analyse soigneuse de cet aspect est nécessaire pour démontrer que la hauteur des culées de l'objet concerné est suffisante au regard des menaces considérées.	

BT.01 Améliorer la conception
Improved design

Cette mesure est pertinente pour la phase de dimensionnement de nouveaux objets. Elle concerne principalement le système statique des ponts. Les systèmes hyperstatiques permettent la redistribution des charges en cas de défaillance d'un certain nombre de sections. Ils sont donc plus résistants aux dommages locaux causés par le feu, une explosion ou un impact.

BT.02 Section transversale des piliers (piles)
Micro-reinforced / ductile high performance concrete (construction material)

La mesure est efficace pour des scénarii avec des impacts mécaniques et des explosions, et est utilisée en premier lieu pour la protection des bâtiments. Si une menace de ce type est identifiée, les éléments structuraux fins sont à éviter ou bien à protéger contre des impacts ayant la valeur retenue pour le dimensionnement.
En cas d'explosions ou d'impacts, la forme des piliers (colonnes) devra être circulaire. Les sections carrées ne sont pas aussi efficaces lorsque les charges agissent dans la direction des éléments de moindre résistance.
Des diamètres et dimensions adéquates pour la protection des colonnes contre une explosion ou un impact doivent être prévus.

BT.03 Béton micro-renforcé/ béton ductile haute performance (matériaux de construction)
Micro-reinforced / ductile high performance concrete (construction material)

Dans le cas d'un objet à grande déformabilité, de l'énergie est absorbée sans dommage (ou alors minime). Cela peut être intéressant pour prévenir les conséquences d'un impact et la protection d'une structure.
Les ponts nouveaux peuvent être construits avec du béton haute résistance plutôt que du béton classique. À dimensions égales, les éléments présentent une plus grande résistance aux effets dynamiques comme les explosions ou les collisions.

Les éléments de soutènement, en particulier l'infrastructure d'un pont, peuvent être protégés en utilisant du béton micro-renforcé et/ou du béton haute-performance contre les impacts d'une explosion.

BT.04 Protection des appuis
Bearing protection

La mesure est efficace pour des scénarii avec des explosions, et est utilisée en premier lieu pour la protection des bâtiments.
La protection des appuis d'un pont peut être importante car ils peuvent être des éléments structuraux critiques d'un pont. Les appuis peuvent être protégés par:

» Des protections physiques pour empêcher l'accès aux appuis.

» Des mesures de prévention – une distance suffisante doit exister entre le lieu de l'explosion potentiel et le bord de l'appui.

» Un accès difficile : les appuis sont situés très haut au-dessus du sol ou bien très bas (culées hautes ou basses)

Il est important de noter qu'aucune protection n'est parfaite. C'est pourquoi, Il faut prévoir une surveillance et des interventions par les services responsables (police…) pour tout réseau ou objet très critique.

BT.05 Dimensionnement pour les contraintes d'une explosion
Design for the explosion load

De nombreux types de ponts peuvent très sensibles aux explosions à certains endroits. Même des explosions relativement faibles peuvent avoir des conséquences disproportionnées en raison d'une réduction de la charge acceptée par certains éléments ou d'une perte de stabilité. Ceci est dû au fait que les codes actuels pour la conception des ouvrages ne prennent pas en compte ces états dans le dimensionnement. C'est pourquoi, les sections et emplacements critiques doivent être définis et vérifiés en fonction des risques identifiés. L'accès à ces composants critiques peut jouer le rôle central dans le cadre de cette étude.

BT.06 Protection contre les collisions (murs de protection, enveloppe de protection)
Collision protection (collision protection walls, collision protection rails)

Pour protéger les piliers du pont contre les collisions, les mesures suivantes peuvent être mises en place:

» Barrières composées de rails (acier ou béton) servant à dévier les véhicules (ou navires) et réduire la vitesse des véhicules (navires) et ainsi la force d'impact.

» Barrières situées à l'avant de l'objet servant à absorber l'énergie de l'impact.

BT.07 Prévention des collisions (glissières de sécurité, espace tampon)
Collision prevention (derailing fences, median space)

Pour prévenir les chocs sur les colonnes d'un pont, les mesures suivantes peuvent être mises en place:

» Rail de sécurité (acier ou béton) servant à rediriger le véhicule (ou navire) et réduire sa vitesse

» Espace central suffisant – notamment en cas d'absence d'autre protection contre une collision.

BT.08 Prévenir le stationnement à proximité des colonnes critiques
Parking in the vicinity of the critical columns prevention

Cette mesure permet de réduire la faisabilité d'une attaque et les dommages potentiels suite à une explosion. De nombreux types de mesures différents peuvent être développés pour différents paramètres CAV:

» Signalétique et obstacles artificiels

» Clôtures et portes

» Barrières de protection

» Mesures architecturales

» Surveillance et intervention etc.

Développer ces mesures d'une manière qui attire l'attention peut avoir des effets négatifs
(les éléments très surveillés peuvent être très attractifs pour une attaque). Pour éviter cet effet, des mesures architecturales peuvent être nécessaires.

MEASURES POUR LES TUNNELS

T.01 Redondance du trafic pour les tunnels
Traffic redundancy for the tunnel

La redondance d'un tunnel signifie la disponibilité d'au moins une des galeries du tunnel après un incident. On distingue deux types de tunnels:

» Tunnel bidirectionnel : la redondance peut être créée par une deuxième galerie. Pour les tunnels bidirectionnels plus longs, la redondance peut être assurée par un tunnel supplémentaire.

» Tunnel unidirectionnel

» Les deux galeries sont à une distance suffisante l'une de l'autre pour que l'effondrement de l'une ne provoque pas l'instabilité structurelle de l'autre. C'est généralement le cas si la méthode de construction est conventionnelle/classique, ou avec l'emploi d'un tunnelier dans des sols très rocheux.

» En cas de conception en tranchée couverte, le mur central entre les deux cellules doit être conçu pour résister aux explosions et contraintes des incendies. Le toit du tunnel doit respecter les critères des contraintes de dimensionnement.

Dans les cas où la redondance d'un objet n'est pas faisable, la redondance au niveau du réseau est proposée pour les objets critiques, attractifs ou vulnérables.

T.02 Catégorisation / Restriction pour les matières dangereuses
DG restriction / categorisation

Cette mesure vise à limiter la faisabilité d'une attaque. Avec cette mesure, la menace d'incendies importants est réduite car le transport de substances dangereuses est restreint et l'événement ne peut pas être déclenché.

T.03 Dimensionnement pour les contraintes d'une explosion
Design for the explosion loads

La mesure est efficace contre les explosions et est utilisée en premier lieu comme mesure de protection structurelle. Elle peut être mise en œuvre au moment de la conception d'un nouveau tunnel.

Exemple : Dimensionnement d'un tunnel en tranchée couverte pour les contraintes de pression interne d'une explosion. Une meilleure résistance peut être obtenue par à la mise en place d'une armature symétrique des travées et piliers ainsi que des angles de cadre susceptibles de supporter des moments de flexion positifs et négatifs. Les caractéristiques de base de la mesure sont:

- Une conception pour des pressions internes élevées,
- Un renforcement symétrique en acier de la structure en béton,
- La création d'angles de cadre ductiles pour des moments de flexion négatifs et positifs,
- L'augmentation de l'épaisseur et du renforcement (localement uniquement),
- La vérification de la capacité résiduelle d'une section transversale (évaluation à la rupture, états limites ultimes – E.L.U.) en tenant compte de toutes les charges.

T.04 Systèmes fixes de lutte contre les incendies
Fixed fire fighting systems

Il s'agit de systèmes dans les tunnels routiers composés d'équipements de lutte contre les incendies montés de manière permanente dans le tunnel, constitués de conduites dotées d'une alimentation permanente en eau ou agent extincteur, et qui permettent lorsqu'ils sont mis œuvre de réduire la production de chaleur et le développement du feu en libérant de l'eau ou l' agent extincteur directement sur l'incendie. Exemples : sprinkler, systèmes à brouillard et écran d'eau.

TT.01 Béton résistant au feu
Fire resistant concrete

De manière générale, le béton est ininflammable mais à contraintes thermiques élevées, la capacité de résistance des armatures peut diminuer si la température interne d'une section de tunnel dépasse 300°C. Ce processus est accéléré en cas d'effritement et de fissuration du béton. Dans le pire des cas, la capacité des armatures pour une section du tunnel est fortement réduite, pouvant engendrer l'effondrement de la voute du tunnel. Le béton résistant au feu prévient la fissuration, réduit et ralentit la diffusion de chaleur dans les éléments structuraux du tunnel.

Les caractéristiques de base de cette mesure sont:

- L'ajout de fibres en polypropylène (PP),
- L'utilisation de granulats adaptés,
- La limitation de la taille maximale des granulats,
- L'utilisation de treillis de renfort supplémentaire pour réduire la fissuration.

TT.02 Revêtement anti-incendie
Fire protection cladding

Le revêtement en béton classique (existant ou neuf) peut être protégé par un revêtement supplémentaire assurant la protection contre les incendies. Différents types de systèmes peuvent être utilisés:

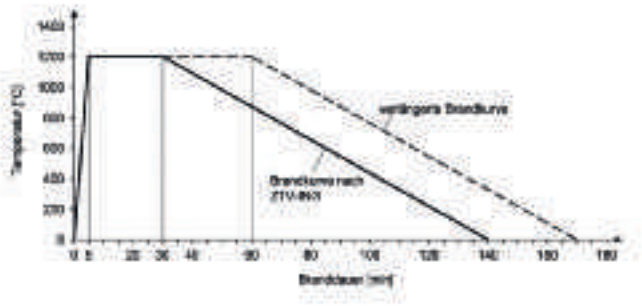
- Pose de plaques ignifuges,
- Projection d'une couche de protection contre les incendies (systèmes de pulvérisation)
- Emploi d'autres matériaux isolants qui réduisent la diffusion de la chaleur dans le revêtement du tunnel.

Le revêtement additionnel agit comme un isolant thermique et réduit la propagation de la chaleur. Il limite l'élévation de la température du béton – la température des armatures reste inférieure à 300°C. Une attention particulière doit cependant être apportée aux inconvénients possibles:

- En cas de contraintes dynamiques, les effets de la pression peuvent endommager le revêtement,
- Le nettoyage peut endommager le revêtement,
- Certains types de mise en œuvre peuvent engendrer des fuites du revêtement en béton voire favoriser l'humidité,
- L'inspection régulière de la structure est empêchée, c'est-à-dire que les fuites et les fissures sont difficiles à déceler derrière les revêtements isolants.

TT.03 Dimensionnement du tunnel pour des contraintes incendie plus élevées
Tunnel design for higher fire loads

La structure du tunnel pourrait être conçue pour une courbe incendie plus contraignante. Par exemple, en augmentant la durée de la phase de feu pleinement constitué de 30 minutes ou augmentant la température maximale atteinte. Un exemple inclus dans la réglementation allemande est présenté ci-dessous.



En conséquence d'une courbe d'incendie prolongée, une structure additionnelle de protection contre les incendies telle qu'un revêtement isolant complémentaire ou l'emploi de béton résistant au feu est souvent préconisé.

TT.04 Structure à enveloppe double
Two shell structure

Dans le cas des tunnels immergés ou bien lorsqu'un tunnel par tunnelier est situé sous le niveau d'une nappe phréatique, les explosions, même de faible puissance, peuvent avoir de lourdes conséquences. Avec une deuxième enveloppe, la redondance structurelle est assurée, même si elle n'est pas nécessaire d'un point de vue statique.

MEASURES POUR LES STRUCTURES ASSOCIÉES

A.01 Protection contre les explosions, projectiles avec des structures en béton (micro-renforcées, ductiles ou haute-performance) Explosions, projectile protection with concrete elements

En cas de petites explosions et tirs de projectiles à proximité d'éléments sensibles ou d'explosions majeures à grande distance des éléments sensibles, la mise en œuvre d'une protection physique résistante peut en réduire sensiblement les conséquences. Cette protection peut être assurée par des murs, revêtements, etc.

A.02 Revêtement anti-incendie
Fire protection cladding

La protection anti-feu passive comprend :

» Des plaques

» De l'habillage et,

» Des enduits.

La mesure ne concerne que les cas d'incendie et est surtout utilisée pour la protection intérieure des bâtiments ou compartiments fermés. Elle est surtout efficace contre les incendies provoqués par l'homme.

A.03 Barrières anti-explosion
Explosion barriers

Les barrières anti-explosion limitent les conséquences des explosions importantes. Dans de nombreux cas, il s'agit d'une menace majeure qui ne peut pas être neutralisée par d'autres mesures.

A.04 Résistance des équipements et redondance
Equipment robustness and redundancy

Il s'agit d'une mesure générale pour toutes parties ou éléments sensibles. Des principes généraux peuvent être donnés; en cas de dommages (enfoncement, cassures physiques…), les éléments doivent être :

» robustes

» redondants

» protégés.

A.05 Prévention du sabotage
Sabotage prevention

La prévention contre les détériorations malveillantes sur les équipements et les éléments fait partie des principaux objectifs de cette mesure. Chaque élément a ses caractéristiques propres et ses procédures d'exploitation, et doit donc faire l'objet d'une analyse séparée.

A.06 Protection contre les collisions (murs de protection)
Collision protection (collision protection walls, collision protection rails)

Pour protéger les éléments sensibles contre les collisions, la mesure suivante peut être mise en œuvre:

» Mettre en place des barrières pour dissiper l'énergie de l'impact à l'avant de l'élément.

A.07 Prévention des collisions (glissière de sécurité, espace tampon)
Collision prevention (derailing fences, median space)

Pour prévenir les collisions avec les éléments sensibles, les mesures suivantes peuvent être mises en œuvre :

» Barrière avec rail de sécurité (acier ou béton) servant à rediriger le véhicule et de ce fait à réduire sa vitesse

» Espace central suffisant pour faire ralentir le véhicule ou rendre son approche impossible.

A.08 Prévention du stationnement à proximité des objets associés
Parking in the vicinity of the accompanying object prevention

Les explosions majeures et les effets de pression qui en résultent (BLEVE) peuvent avoir de graves impacts même si la distance est relativement grande entre l'explosion et les objets. D'autre part, même des explosions relativement faibles à proximité d'un objet peuvent avoir des conséquences disproportionnées sur l'infrastructure et la durée de sa reconstruction. Un autre effet positif de cette mesure est de limiter les possibilités d'observation des activités et de l'infrastructure par des personnes non-autorisées.

De nombreuses formes de mesures peuvent être envisagées pour prévenir ces effets:

» Signalétique et obstacles artificiels

» Clôtures et portes

» Barrières de protection

» Mesures architecturales

» Surveillance et intervention etc.

Durant la conception de ces mesures, l'excitation visuelle doit être vérifiée et des mesures compensatoires doivent être prises si nécessaire. La protection de l'infrastructure peut avoir des effets négatifs; les éléments très surveillés peuvent être très attractifs pour une attaque. Dans ce cas, des mesures architecturales supplémentaires peuvent être utilisées.

A.09 Systèmes fixes de lutte contre les incendies
Fixed fire fighting systems

Cette mesure est une protection active pour prévenir le développement d'un incendie dans sa phase de croissance ou pour arrêter la progression d'un incendie déclaré dans un espace fermé. Aussi, la détection des incendies est cruciale. Une méthode actuellement bien établie est l'extinction automatique d'un incendie avec du gaz. D'autres systèmes fixes de lutte contre l'incendie sont possibles, il est toutefois nécessaire d'en étudier l'efficacité en cas d'attaque.

MANUEL DE SECURITE POUR LES INFRASTRUCTURES ROUTIERES EUROPENNES

Ce manuel a été élaboré par le consortium du projet européen SecMan,

Coordonné par l'Institut fédéral de la recherche routière (BASt) (Allemagne)

En collaboration avec
ILF Consulting Engineers (Autriche),

ELEA iC Consulting Engineers (Slovénie) et

DARS Motorway Company (Slovénie).

SecMan a été financé par le programme CIPS « Prévention, préparation et gestion des conséquences en matière de terrorisme et autres risques liés à la sécurité » de la direction générale des affaires intérieures de la commission européenne.

Le manuel a été préparé par:
Jakob Haardt (Institut fédéral de la recherche routière)
Harald Kammerer (ILF Consulting Engineers)
Les participants à ce manuel sont :
Miha Hafner (ELEA iC Consulting Engineers)
Drago Dolenc (DARS Motorway Company)
Le manuel a été révisé par :
Jürgen Krieger (Institut fédéral de la recherche routière)
Ingo Kaundinya (Institut fédéral de la recherche routière)
Bernhard Kohl (ILF Consulting Engineers)
Marko Žibert (ELEA iC Consulting Engineers)

Le manuel est aussi disponible :
1. en ligne sur : www.secman-project.eu
2. prêt à être imprimé en allemand, français et espagnol.
3. Pour acheter une version papier, merci de contacter :
Institut fédéral de la recherche routière
Section B3
Brüderstraße 53
51427 Bergisch Gladbach
Allemagne
0049-2204-43858
secman@bast.de
Droits d'auteurs
Consortium SecMan, 2013

Avis de non-responsabilité:
Tous les avis, résultats, conclusions et conseils indiqués dans cette publication appartiennent aux auteurs et ne reflètent pas nécessairement les visions de leurs organisations ou entreprises. Ces résultats sont donnés à titre indicatif uniquement et les auteurs ne sont pas responsables des dommages ou coûts résultant de l'application de la méthodologie proposée.

Les images appartiennent à l'Institut fédéral de la recherche routière.

Les diagrammes et les tableaux appartiennent au consortium SecMan.

Le consortium souhaiterait remercier la direction générale des affaires intérieures de l'UE pour avoir financé le projet SecMan et soutenu sa mise en place. De plus, les auteurs aimeraient remercier les participants du comité consultatif, des séminaires et de l'enquête du projet SecMan, notamment pour les informations intéressantes des sous-traitants pendant toute la durée du projet. Par ailleurs, les fournisseurs des données des infrastructures routières ont également participé à la validation de la méthodologie.